United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, Committee on Government Reform, House of Representatives

For Release on Delivery
Expected at
10:00 a.m. EDT
Wednesday,
July 24, 2002

CRITICAL INFRASTRUCTURE PROTECTION

Significant Challenges Need to Be Addressed

Statement of Robert F. Dacey
Director, Information Security Issues

Report Documentation Page

Report Date	Report Type	Dates Covered (from... to)
00JUL2002	N/A	-

Title and Subtitle CRITICAL INFRASTRUCTURE PROTECTION: Significant Challenges Need to Be Addressed	**Contract Number**
	Grant Number
	Program Element Number
Author(s)	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) U.S. General Accounting Office 441 G Street NW, Room LM Washington, D.C. 20548	**Performing Organization Report Number** GAO-02-961t
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Sponsor/Monitor's Acronym(s)**
	Sponsor/Monitor's Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes	
Abstract see report	
Subject Terms	
Report Classification unclassified	**Classification of this page** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** SAR
Number of Pages 64	

GAO
Accountability★Integrity★Reliability

Highlights

CRITICAL INFRASTRUCTURE PROTECTION
Significant Challenges Need to Be Addressed

Highlights of GAO-02-961T, testimony before the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, House Committee on Government Reform.

Why GAO Did This Study

The explosion in computer interconnectivity, while providing great benefits, also poses enormous risks. Terrorists or hostile foreign states could launch computer-based attacks on critical systems to severely damage or disrupt national defense or other critical operations.

Presidential Decision Directive 63 and Executive Order 13231, issued in 1998 and 2001, respectively, call for various actions to improve our nation's critical infrastructure protection (CIP), including establishing partnerships between the government and the private sector. CIP involves activities that enhance the security of our nation's cyber and physical public and private infrastructure that are essential to national security, national economic security, and/or national public health and safety.

The President's national strategy for homeland security, issued last week, identifies protecting critical infrastructures and intelligence and warning, a critical CIP component, as two of six mission areas and expands our nation's approach to cover additional sectors of our economy (see graphic). At the subcommittee's request, GAO discussed challenges the nation faces in protecting our critical infrastructures and addressing federal information security.

What GAO Found

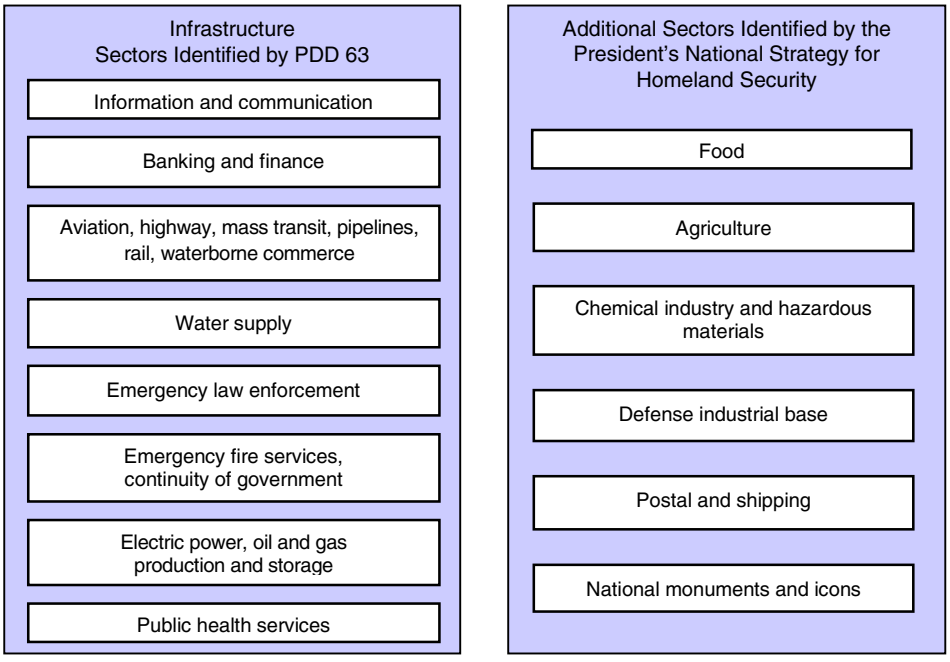
Prior GAO work has identified and made recommendations concerning several CIP challenges that need to be addressed:

- *Developing a national critical infrastructure protection strategy.* A more complete strategy is needed to define specific roles, responsibilities, and relationships for all CIP organizations and to establish objectives, timeframes, and performance measures. The President's national strategy calls for more detailed CIP plans.

- *Improving analytical and warning capabilities.* More robust analytical and warning capabilities are still needed to identify threats and provide timely warnings, including an effective methodology for strategic analysis and framework for collecting needed threat and vulnerability information.

- *Improving information sharing.* Information sharing needs to be enhanced both within the government and between the federal government and the private sector.

- *Addressing pervasive weaknesses in federal information security.* A comprehensive strategy for improving federal information security is needed, in which roles and responsibilities are clearly delineated, appropriate guidance is given, regular monitoring is undertaken, and security information and expertise are shared to maximize their value.



Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to discuss the challenges that our nation faces concerning critical infrastructure protection (CIP) and federal information security. CIP involves activities that enhance the security of our nation's cyber and physical public and private infrastructure that are essential to national security, national economic security, and/or national public health and safety. Federal agencies and other public and private entities rely extensively on computerized systems and electronic data to support their missions. Accordingly, the security of these systems and data is essential to avoiding disruptions in critical operations, data tampering, fraud, and inappropriate disclosure of sensitive information. Further, protecting against computer-based attacks on critical infrastructures is an important aspect of homeland security. Earlier this month, we testified on the proposed transfer of certain government agencies associated with protecting our nation's critical infrastructures to the Department of Homeland Security.[1] Congress has held numerous hearings on this subject, passed legislation, and issued reports[2] that have been instrumental in ensuring appropriate oversight and focus.

Today, as requested, I will provide an overview of the federal government's approach to protecting our nation's critical infrastructures that is described in Presidential Decision Directive (PDD) 63, Executive Order 13231, and the newly issued national strategy for homeland security.[3] I will also provide an overview of cyber threats and vulnerabilities. Next, I will discuss the challenges, identified in prior GAO work, that the nation continues to face in implementing CIP and consequently in protecting our homeland, as well as protecting federal information systems. These challenges are (1) developing a more complete national CIP strategy, (2) improving analysis and warning capabilities, (3) building on information sharing efforts, and (4) addressing the pervasive nature of federal information security weaknesses.

In preparing this testimony, we relied on prior GAO reports and testimonies on CIP, information security, and national preparedness, among others. We also met with officials at the Department of Commerce's Critical Infrastructure Assurance Office and the Federal Bureau of Investigation's (FBI) National Infrastructure Protection Center

[1] U.S. General Accounting Office, *Critical Infrastructure Protection: Significant Homeland Security Challenges Need To Be Addressed* GAO-02-918T (Washington, D.C.: July 9, 2002).

[2] *Security in the Information Age, New Challenges, New Strategies*, Joint Economic Committee, United States Congress, May 2002.

[3] *National Strategy for Homeland Security*, Office of Homeland Security, July 2002.

to follow up on prior recommendations and to discuss their proposed move to the new department. We also reviewed the national strategy for homeland security released last week. Our work was performed in accordance with generally accepted government auditing standards.

Results in Brief

We have identified and made numerous recommendations over the last several years concerning several CIP and federal information security challenges that need to be addressed. For each of these challenges, improvements have been made and continuing efforts are in progress. However, much more is needed to address them. These challenges include:

- *Developing a national CIP strategy.* A more complete strategy is needed that will address specific roles, responsibilities, and relationships for all CIP entities; clearly define interim objectives and milestones; set time frames for achieving objectives; establish performance measures; and include all relevant sectors. Last week, we issued a report that further highlights the importance of coordinating the many entities involved in cyber CIP efforts.[4] The President's national strategy for homeland security, also issued last week, calls for interim cyber and physical infrastructure protection plans by September 2002 and a comprehensive national infrastructure plan to be completed by the Department of Homeland Security. The strategy does not indicate when this comprehensive plan will be completed. Until a comprehensive and coordinated strategy is developed for all CIP efforts, our nation risks not having a consistent and appropriate structure to deal with the growing threat of computer-based attacks on its critical infrastructure.
- *Improving analysis and warning capabilities.* More robust analysis and warning capabilities, including an effective methodology for strategic analysis and framework for collecting needed threat and vulnerability information, are still needed to identify threats and provide timely warnings. Such capabilities need to address both cyber and physical threats. The national strategy for homeland security calls for major initiatives to improve our nation's analysis and warning capabilities that include enhancing existing capabilities at the FBI and building new capabilities at the proposed Department of Homeland Security.
- *Improving information sharing on threats and vulnerabilities.* Information sharing needs to be enhanced both within the government and between the federal government and the private sector and state and local governments. The national strategy for homeland security identifies

[4]U.S. General Accounting Office, *Critical Infrastructure Protection: Federal Efforts Require a More Coordinated and Comprehensive Approach for Protecting Information Systems,* GAO-02-474 (Washington, D.C.: July 15, 2002).

partnering with nonfederal entities as a major initiative and discusses the need to integrate information sharing within the federal government and among federal, state, and local governments and private industry. The strategy also discusses the need to use available public policy tools, such as grants.

- *Addressing pervasive weaknesses in federal information security.* Because of our government's and our nation's reliance on interconnected computer systems to support critical operations and infrastructures, poor information security could have potentially devastating implications for our country. Despite the importance of maintaining the integrity, confidentiality, and availability of important federal computerized operations, federal computer systems have significant pervasive information security weaknesses. A comprehensive strategy for improving federal information security is needed, in which roles and responsibilities are clearly delineated, appropriate guidance is given, regular monitoring is undertaken, and security information and expertise are shared to maximize their value.

Although the national strategy for homeland security acknowledges the need to address many of the challenges discussed above, much work remains to successfully implement it. The President's draft legislation on the creation of a Department of Homeland Security would create an information analysis and infrastructure protection division to address many of these challenges. Earlier this month, we testified on the potential benefits and challenges of the proposed transfer. In addition, the Comptroller General has recently testified on key issues related to the successful implementation of, and transition to, the new Department of Homeland Security.[5]

Critical Infrastructure Protection Policy Has Been Evolving Since the Mid-1990's

Federal awareness of the importance of securing our nation's critical infrastructures, which underpin our society, economy, and national security, has been evolving since the mid-1990's. Over the years, a variety of working groups have been formed, special reports written, federal policies issued, and organizations created to address the issues that have been raised. In October 1997, the President's Commission on Critical Infrastructure Protection issued its report,[6] which described the potentially devastating implications of poor information security from a national perspective. The report recommended several measures to achieve a higher level of critical infrastructure protection, including infrastructure protection through industry cooperation and information

[5]U.S. General Accounting Office, *Homeland Security: Critical Design and Implementation Issues,* GAO-02-957T (Washington D.C.: July 17, 2002).

[6]*Critical Foundations: Protecting America's Infrastructures*, Report of the President's Commission on Critical Infrastructure Protection (Oct. 1997).

sharing, a national organization structure, a revised program of research and development, a broad program of awareness and education, and reconsideration of laws related to infrastructure protection. The report stated that a comprehensive effort would need to "include a system of surveillance, assessment, early warning, and response mechanisms to mitigate the potential for cyberthreats." It said that the FBI had already begun to develop warning and threat analysis capabilities and urged it to continue in these efforts. In addition, the report noted that the FBI could serve as the preliminary national warning center for infrastructure attacks and provide law enforcement, intelligence, and other information needed to ensure the highest quality analysis possible.

In 1998, the President issued PDD 63, which described a strategy for cooperative efforts by government and the private sector to protect the physical and cyber-based systems essential to the minimum operations of the economy and the government. PDD 63 called for a range of actions intended to improve federal agency security programs, improve the nation's ability to detect and respond to serious computer-based and physical attacks, and establish a partnership between the government and the private sector. The directive called on the federal government to serve as a model of how infrastructure assurance is best achieved and designated lead agencies to work with private-sector and government organizations. Further, it established CIP as a national goal and stated that, by the close of 2000, the United States was to have achieved an initial operating capability to protect the nation's critical infrastructures from intentional destructive acts and, no later than 2003, an enhanced capability.

To accomplish its goals, PDD 63 designated and established organizations to provide central coordination and support, including

- the Critical Infrastructure Assurance Office (CIAO), an interagency office housed in the Department of Commerce, which was established to develop a national plan for CIP on the basis of infrastructure plans developed by the private sector and federal agencies;
- the National Infrastructure Protection Center (NIPC), an organization within the FBI, which was expanded to address national-level threat assessment, warning, vulnerability, and law enforcement investigation and response; and

- the National Infrastructure Assurance Council, which was established to enhance the partnership of the public and private sectors in protecting our critical infrastructures.[7]

To ensure coverage of critical sectors, PDD 63 also identified eight private-sector infrastructures and five special functions. The infrastructures are (1) information and communications; (2) banking and finance; (3) water supply; (4) aviation, highway, mass transit, pipelines, rail, and waterborne commerce; (5) emergency law enforcement; (6) emergency fire services and continuity of government; (7) electric power and oil and gas production and storage; and (8) public health services. The special functions are (1) law enforcement and internal security, (2) intelligence, (3) foreign affairs, (4) national defense, and (5) research and development. For each of the infrastuctures and functions, the directive designated lead federal agencies, known as sector liaisons, to work with their counterparts in the private sector, known as sector coordinators. For example, the Department of the Treasury is responsible for working with the banking and finance sector, and the Department of Energy is responsible for working with the electrical power industry. Similarly, regarding special function areas, the Department of Defense (DOD) is responsible for national defense, and the Department of State is responsible for foreign affairs.

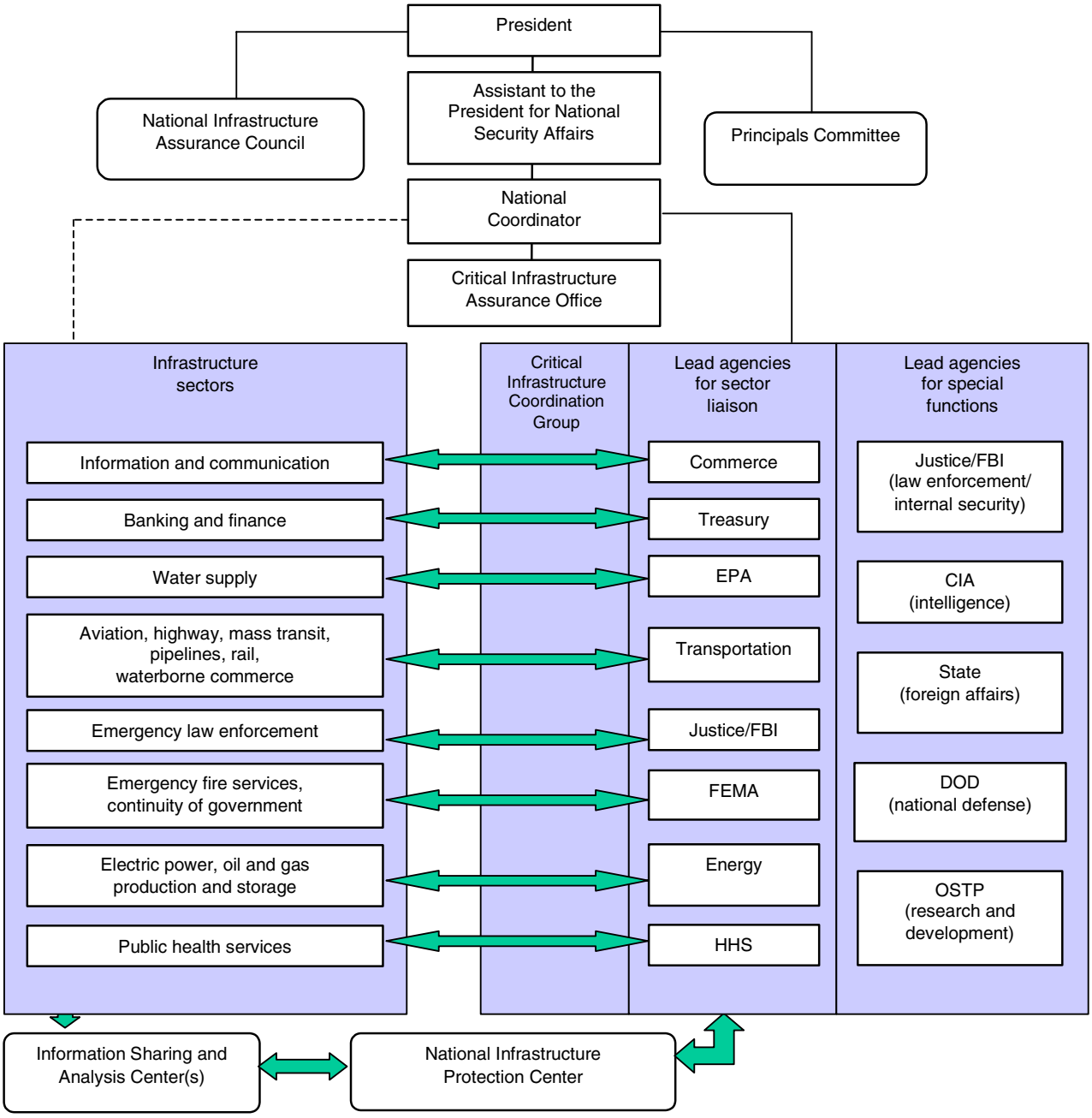
PDD 63 called for a range of actitivites intended to establish a partnership between the public and private sector to ensure the security of infrastructures essential to the operations of the government and the economy. It required that the sector liaison and the sector coordinator work with each other to address problems related to CIP for their sector. In particular, PDD 63 required them to (1) develop and implement a vulnerability awareness and education program and (2) contribute to a sectoral National Infrastructure Assurance Plan by

- assessing the vulnerabilities of the sector to cyber or physical attacks;
- recommending a plan to eliminate significant vulnerabilities;
- proposing a system for identifying and preventing major attacks; and
- developing a plan for alerting, containing, and rebuffing an attack in progress and then, in coordination with the Federal Emergency Management Agency as appropriate, rapidly reconstitute minimum essential capabilities in the aftermath of an attack.

[7]Executive Order 13231 replaces this council with the National Infrastructure Advisory Council.

To facilitate private-sector participation, PDD 63 also encouraged the voluntary creation of information sharing and analysis centers (ISACs) that could serve as mechanisms for gathering, analyzing, and appropriately sanitizing and disseminating information to and from infrastructure sectors and the federal government through NIPC. Figure 1 displays a high-level overview of the organizations with CIP responsibilities as outlined by PDD 63.

Figure 1: Organizations with CIP Responsibilities as Outlined by PDD 63



Note: In February 2001, the Critical Infrastructure Coordination Group was replaced by the Information Infrastructure Protection and Assurance Group under the Policy Coordinating Committee on Counter-terrorism and National Preparedness. In October 2001, the National Infrastructure Assurance Council was replaced by the National Infrastructure Advisory Council, and cyber CIP functions performed by the national coordinator were assigned to the chair of the President's Critical Infrastructure Protection Board.

Source: CIAO.

In January 2000 the White House issued its *National Plan for Information Systems Protection*.[8] The national plan provided a vision and framework for the federal government to prevent, detect, respond to, and protect the nation's critical cyber-based infrastructure from attack and reduce existing vulnerabilities by complementing and focusing existing federal computer security and information technology requirements. Subsequent versions of the plan were expected to (1) define the roles of industry and state and local governments working in partnership with the federal government to protect physical and cyber-based infrastructures from deliberate attack and (2) examine the international aspects of CIP.

In October 2001, President Bush signed Executive Order 13231, establishing the President's Critical Infrastructure Protection Board to coordinate cyber-related federal efforts and programs associated with protecting our nation's critical infrastructures. The Special Advisor to the President for Cyberspace Security chairs the board. Executive Order 13231 tasks the board with recommending policies and coordinating programs for protecting CIP-related information systems. The executive order also established 10 standing committees to support the board's work on a wide range of critical information infrastructure efforts. The board is intended to coordinate with the Office of Homeland Security in activities relating to the protection of and recovery from attacks against information systems for critical infrastructure, including emergency preparedness communications that were assigned to the Office of Homeland Security by Executive Order 13228, dated October 8, 2001. According to Executive Order 13231, the board recommends policies and coordinates programs for protecting information systems for critical infrastructure, including emergency preparedness communications and the physical assets that support such systems. The Special Advisor reports to the Assistant to the President for National Security Affairs and to the Assistant to the President for Homeland Security. In addition, the chair coordinates with the Assistant to the President for Economic Policy on issues relating to private-sector systems and economic effects and with the Director of the Office of Management and Budget (OMB) on issues relating to budgets and the security of federal computer systems. In addition, Executive Order 13231 reiterated the importance and voluntary nature of the ISACs but did not suggest additional activities for the ISACs.

Last week, the President issued the national strategy for homeland security to "mobilize and organize our nation to secure the United States homeland from terrorist attacks." According to the strategy, the primary objectives of homeland security in order of priority are to (1) prevent terrorist attacks within the United States, (2) reduce America's

[8]The White House, *Defending America's Cyberspace: National Plan for Information Systems Protection: Version 1.0: An Invitation to a Dialogue* (Washington, D.C.: 2000).

vulnerability to terrorism, and (3) minimize the damage and recover from attacks that do occur. The strategy identifies critical infrastructure and intelligence and warning, a critical component of CIP, as two of six mission areas; the strategy states that if terrorists attack one or more pieces of our critical infrastructure, they may disrupt entire systems and cause significant damage to the nation. The other four mission areas are border and transportation security, domestic terrorism, defending against catastrophic terrorism, and emergency preparedness and response.

Implementing PDD 63 Has Not Been Completely Successful

Both GAO and the inspectors general have issued reports highlighting concerns about PDD 63 implementation. As we reported in September 2001, efforts to perform substantive, comprehensive analyses of infrastructure sector vulnerabilities and the development of related remedial plans had been limited. Further, a March 2001 report by the President's Council on Integrity and Efficiency and the Executive Council on Integrity and Efficiency (PCIE/ECIE) identified significant deficiencies in federal agencies' implementation of PDD 63 requirements to (1) establish plans for protecting their own critical infrastructure that were to be implemented within 2 years, or by December 2000, and (2) develop procedures and conduct vulnerability assessments.[9] Specifically,

- many agency CIP plans were incomplete, and some agencies had not developed such plans;
- most agencies had not completely identified their mission-essential infrastructure assets; and
- few agencies had completed vulnerability assessments of their minimum essential infrastructure assets or developed remediation plans.

Our subsequent review of PDD 63-related activities at eight lead agencies found similar problems, although some agencies had made progress since their respective inspectors general reviews.[10] Further, OMB reported in February 2002 that it planned to direct all large agencies to undertake a Project Matrix review to identify critical infrastructure assets and their interdependencies with other agencies and the private sector.[11]

[9]The PCIE primarily is composed of the presidentially appointed inspectors general and the ECIE is primarily composed of the agency head-appointed inspectors general. In November 1999, PCIE and ECIE formed a working group to review the adequacy of federal agencies' implementation of PDD 63. The March 2001 report is based on reviews by 21 inspectors general of their respective agencies' PDD 63 planning and assessment activities.

[10]GAO-01-822, September 20, 2001.

[11]Project Matrix is a CIAO methodology that identifies all critical assets, nodes, networks, and associated infrastructure dependencies and interdependencies.

We identified several other factors that had impeded the efforts of federal agencies to comply with PDD 63. First, no clear definitions had been developed to guide development and implementation of agency plans and measure performance. For example, PDD 63 established December 2000 as the deadline for achieving an initial operating capability and May 2003 for achieving full operational capability of key functions. However, the specific capabilities to be achieved at each milestone had not been defined. The PCIE/ECIE report noted that agencies had used various interpretations of initial operating capability and stated that, without a definition, there is no consistent measure of progress toward achieving full security preparedness. In addition, several agency officials said that funding and staffing constraints contributed to their delays in implementing PDD 63 requirements. Further, the availability of adequate technical expertise to provide information security has been a continuing concern to agencies.

Cyber Threats Are Increasing and Infrastructure Sectors Are Vulnerable

Dramatic increases in computer interconnectivity, especially in the use of the Internet, are revolutionizing the way our government, our nation, and much of the world communicate and conduct business. The benefits have been enormous. Vast amounts of information are now literally at our fingertips, facilitating research on virtually every topic imaginable; financial and other business transactions can be executed almost instantaneously, often on a 24-hour-a-day basis; and electronic mail, Internet web sites, and computer bulletin boards allow us to communicate quickly and easily with a virtually unlimited number of individuals and groups.

In addition to such benefits, however, this widespread interconnectivity poses significant risks to our computer systems and, more important, to the critical operations and infrastructures they support. For example, telecommunications, power distribution, water supply, public health services, and national defense (including the military's warfighting capability), law enforcement, government services, and emergency services all depend on the security of their computer operations. The speed and accessibility that create the enormous benefits of the computer age likewise, if not properly controlled, allow individuals and organizations to inexpensively eavesdrop on or interfere with these operations from remote locations for mischievous or malicious purposes, including fraud or sabotage.

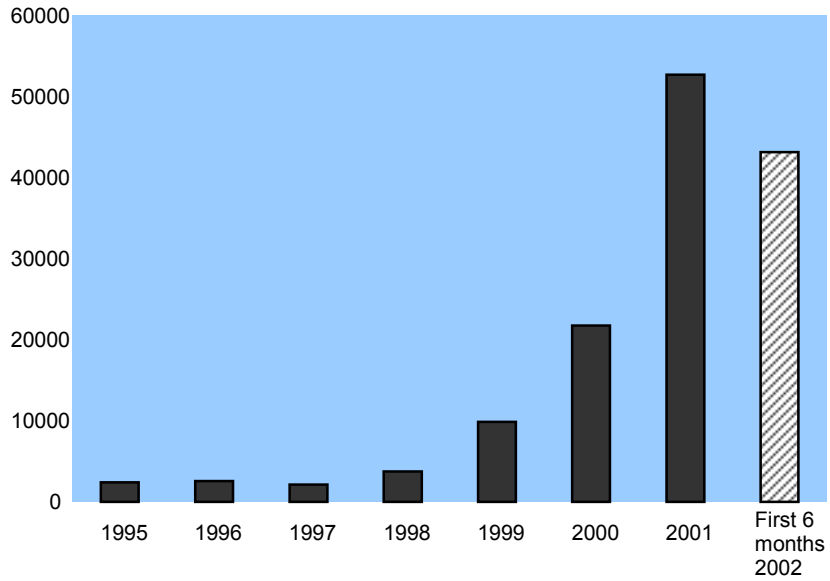
Government officials are increasingly concerned about attacks from individuals and groups with malicious intent, such as crime, terrorism, foreign intelligence gathering, and acts of war. According to the FBI, terrorists, transnational criminals, and intelligence services are quickly

becoming aware of and using information exploitation tools such as computer viruses, Trojan horses, worms, logic bombs, and eavesdropping sniffers that can destroy, intercept, degrade the integrity of, or deny access to data. As greater amounts of money are transferred through computer systems, as more sensitive economic and commercial information is exchanged electronically, and as the nation's defense and intelligence communities increasingly rely on commercially available information technology, the likelihood increases that information attacks will threaten vital national interests. In addition, the disgruntled organization insider is a significant threat, since such individuals often have knowledge that allows them to gain unrestricted access and inflict damage or steal assets without possessing a great deal of knowledge about computer intrusions.

Reports of attacks and disruptions abound. The 2002 report of the "Computer Crime and Security Survey," conducted by the Computer Security Institute and the FBI's San Francisco Computer Intrusion Squad, showed that 90 percent of respondents (primarily large corporations and government agencies) had detected computer security breaches within the last 12 months. In addition, the number of computer security incidents reported to the CERT® Coordination Center rose from 9,859 in 1999 to 52,658 in 2001 and 43,136 for just the first six months of 2002.[12] And these are only the reported attacks. The CERT® Coordination Center estimates that as much as 80 percent of actual security incidents go unreported, in most cases because the organization was unable to recognize that its systems had been penetrated or because there were no indications of penetration or attack. Figure 2 shows the number of incidents reported to the CERT® Coordination Center from 1995 through the first six months of 2002.

[12]CERT® Coordination Center (CERT-CC) is a center of Internet security expertise located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University.

Figure 2: Information Security Incidents Reported to Carnegie-Mellon's CERT® Coordination Center: 1995-the first six months of 2002



Source: Carnegie-Mellon's CERT® Coordination Center

Since the September 11 attacks, warnings of the potential for terrorist cyber attacks against our critical infrastructures have also increased. For example, earlier this year, the Special Advisor to the President for Cyberspace Security stated in a Senate briefing that although to date none of the traditional terrorist groups such as al Qaeda have used the Internet to launch a known attack on the United States infrastructure, information on computerized water systems was recently discovered on computers found in al Qaeda camps in Afghanistan. Further, in his October congressional testimony, Governor James Gilmore, former Governor of the Commonwealth of Virginia and Chairman of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (commonly known as the "Gilmore Commission"), warned that systems and services critical to the American economy and the health of our citizens—such as banking and finance, "just-in-time" delivery systems for goods, hospitals, and state and local emergency services—could all be shut down or severely handicapped by a cyber attack or a physical attack against computer hardware.[13] The national strategy for homeland security states that terrorist groups are already

[13]Testimony of Governor James S. Gilmore III, former Governor of the Commonwealth of Virginia and Chairman of the Advisory Panel to Assess the Capabilities for Domestic Response to Terrorism Involving Weapons of Mass Destruction before the House Science Committee, October 17, 2001.

exploiting new information technology and the Internet to plan attacks, raise funds, spread propaganda, collect information, and communicate securely.

Each of the sectors' critical infrastructures is vulnerable in varying degrees to natural disasters, component failures, human negligence, and willful misconduct. Several examples are highlighted below.

- In 1997, the *Report of the President's Commission on Critical Infrastructure Protection* stated that treated water supplies did not have adequate physical protection to mitigate the threat of chemical or biological contamination, nor was there technology available to allow for detecting, identifying, measuring, and treating highly toxic, waterborne contaminants. It added that cyber vulnerabilities include the increasing reliance on Supervisory Control and Data Acquisition (SCADA)[14] systems used to monitor and control equipment for control of the flow and pressure of water supplies. Several weeks ago, the President of the Association of Metropolitan Water Agencies testified that water utilities are increasingly reliant on information systems to control many aspects of water treatment and distribution and stressed the importance of conducting research into methodologies and technologies to detect, prevent, and respond to acts of terrorism against drinking water systems. In addition, on January 30, 2002, NIPC issued an information bulletin on terrorist interest in water supply and SCADA systems. It stated that a computer that belonged to an individual with indirect links to bin Laden contained structural architecture computer programs that suggested that the individual was interested in structural engineering as it related to dams and other water-retaining structures. The bulletin further stated that U.S. law enforcement and intelligence agencies have received indications that al Qaeda members have sought information on SCADA systems that is available on multiple SCADA-related web sites.
- The President's 1997 Commission also reported on the physical vulnerabilities for electric power related to substations, generation facilities, and transmission lines. It further added that the widespread and increasing use of SCADA systems for control of energy systems provides increasing capability to cause serious damage and disruption by cyber means. Riptech, a Virginia-based security firm, recently released an Internet security threat report for the period of January 1, 2002, to June 30, 2002, that was based on information from a sample of its client

[14]SCADA systems allow utility operators to monitor and control processes that are distributed among various remote sites. This connectivity offers increased accessibility and ease of operations for legitimate users, but also could expose the utility to cyber intruders.

organizations.[15] Riptech concluded that companies in the energy industry, along with financial services and high-tech companies, experience the highest rate of overall attack activity. According to the study, power and energy firms received an average of 1,280 attacks per company and 70 percent of them had at least one severe attack during the period studied. Riptech has also reported on the vulnerabilities of SCADA systems.

- In February 2002, the National Security Telecommunications Advisory Committee and the National Communications System released a document, *An Assessment of the Risk to the Security of the Public Network*, relating to the vulnerabilities of the telecommunications sector. This report concludes that (1) the overall vulnerability of the public network to electronic intrusion has increased, (2) government and industry organizations have worked diligently to improve protection measures, (3) the threat to the public network continues to grow as it becomes a more valuable target and the intruder community develops more sophisticated capabilities to launch attacks against it, and (4) continuing trends in law enforcement and legislation have increased the ability of the government and the private sector to deter the threat of intrusion. The report says that the implementation of packet-based next-generation network technologies, including wireless, and their convergence with traditional networks have introduced even more vulnerabilities into the public network.

  Not only is cyber protection of our critical infrastructures important in and of itself, but a physical attack in conjunction with a cyber attack has recently been highlighted as a major concern. In fact, NIPC has stated that the potential for compound cyber and physical attacks, referred to as "swarming attacks," is an emerging threat to the U.S. critical infrastructure. As NIPC reports, the effects of a swarming attack include slowing or complicating the response to a physical attack. For example, cyber attacks can be used to delay the notification of emergency services and to deny the resources needed to manage the consequences of a physical attack. In addition, a swarming attack could be used to worsen the effects of a physical attack. For example, a cyber attack on a natural gas distribution pipeline that opens safety valves and releases fuels or gas in the area of a planned physical attack could enhance the force of the physical attack.

  Understanding the many interdependencies between sectors is also critical to the success of protecting our national infrastructures. According to a report by the CIP Research and Development Interagency Working

[15]For the 6-month period, Riptech analyzed firewall logs and intrusion detection system alerts. From these initial data, more than 1 million possible attacks were isolated and more than 180,000 confirmed.

Group,[16] the effect of interdependencies is that a disruption in one infrastructure can spread and cause appreciable impact on other infrastructures.[17] The report also stated that understanding interdependencies is important because the proliferation of information technology has made the infrastructures more interconnected, and the advent of competition, "just in time" business, and mergers among infrastructure owners and operators have eroded spare infrastructure capacity. In congressional testimony earlier this month, the director of Sandia National Laboratories' Infrastructure and Information Systems Center stated that these interdependencies make it difficult to identify critical nodes, vulnerabilities, and optimized mitigation strategies.

The Nation Faces Ongoing CIP Challenges

For years, we have reported on and made numerous recommendations to improve the protection of our critical infrastructures and federal information systems. Specific challenges that the nation faces include developing a more complete national CIP strategy, improving analysis and warning capabilities, improving information sharing, and addressing pervasive weaknesses in federal information security.

National CIP Strategy Needs to Be Developed

A clearly defined strategy is essential for defining the relationships among all CIP organizations to ensure that the approach is comprehensive and well coordinated. An underlying issue in the implementation of PDD 63 is that no national strategy yet exists that clearly delineates the roles and responsibilities of federal and nonfederal CIP entities and defines interim objectives.[18] We have reported since 1998 on the need for such a strategy. Just last week we issued a report making additional recommendations about what should be included in this strategy.[19] The national strategy for homeland security calls for interim cyber and physical infrastructure protection plans by September 2002 and a comprehensive national infrastructure plan to be completed by the Department of Homeland Security. The strategy does not indicate a date when this comprehensive plan is to be issued.

[16]The CIP Research and Development Interagency Working Group was established in March 1998 to develop and sustain a roadmap on what technologies should be pursued to reduce vulnerabilities of and counter threats to our critical infrastructures.

[17]*Report on the Federal Agenda in Critical Infrastructure Protection Research and Development, Research Vision, Objectives, and Programs,* CIP Research and Development Interagency Working Group, January 2001.

[18]GAO-01-822, September 20, 2001.

[19]GAO-02-474, July 15, 2002.

GAO Has Long Recognized the Need for a National CIP Strategy

In September 1998, we reported that developing a governmentwide strategy that clearly defined and coordinated the roles of new and existing federal entities was important to ensure governmentwide cooperation and support for PDD 63.[20] At that time, we recommended that OMB and the Assistant to the President for National Security Affairs ensure such coordination.

In January 2000, the President issued *Defending America's Cyberspace: National Plan for Information Systems Protection: Version 1.0: An Invitation to a Dialogue* as a first major element of a more comprehensive effort to protect the nation's information systems and critical assets from future attacks. The plan proposed achieving the twin goals of making the U.S. government a model of information security and developing a public/private partnership to defend our national infrastructures by achieving three crosscutting infrastructure protection objectives:

- minimizing the possibility of significant and successful attacks;
- identifying, assessing, containing, and quickly recovering from an attack; and
- creating and building strong foundations, including people, organizations, and laws, for preparing, preventing, detecting and responding to attacks.

However, this plan focused largely on federal cyber CIP efforts, saying little about the private-sector role. Subsequently, in July 2000, we reiterated the importance of defining and clarifying organizational roles and responsibilities, noting that numerous federal entities were collecting, analyzing, and disseminating data or guidance on computer security vulnerabilities and incidents and that clarification would help ensure a common understanding of (1) how the activities of these many organizations interrelate; (2) who should be held accountable for their success or failure; and (3) whether such activities will effectively and efficiently support national goals.[21]

A May 2001 White House press statement announced that the administration was reviewing how it was organized to deal with

[20]U.S. General Accounting Office, *Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk*, GAO/AIMD-98-92 (Washington, D.C.: Sept. 23, 1998).

[21]U.S. General Accounting Office, *Critical Infrastructure Protection: Challenges to Building a Comprehensive Strategy for Information Sharing and Cooperation*, GAO/T-AIMD-00-268 (Washington, D.C.: July 26, 2000).

information security issues and that recommendations would be made on how to structure an integrated approach to cyber security and CIP. Specifically, the announcement stated that the White House, federal agencies, and private industry had begun to collaboratively prepare a new version of a "national plan for cyberspace security and critical infrastructure protection" and review how the government is organized to deal with information security issues.

In September 2001, we reported that agency questions had surfaced regarding specific roles and responsibilities of entities involved in cyber CIP and the timeframes within which CIP objectives are to be met, as well as guidelines for measuring progress.[22] Accordingly, we made several recommendations to supplement those we had made in the past, including those regarding NIPC. Specifically, we recommended that the Assistant to the President for National Security Affairs ensure that the federal government's strategy to address computer-based threats define

- specific roles and responsibilities of organizations involved in CIP and related information security activities;
- interim objectives and milestones for achieving CIP goals and a specific action plan for achieving these objectives, including implementing vulnerability assessments and related remedial plans; and
- performance measures for which entities can be held accountable.

National Strategy Needs to Define Relationships among the Key CIP Organizations and Include All Sectors

In a report issued last week, we identified at least 50 organizations involved in national or multiagency cyber CIP efforts.[23] These entities include 5 advisory committees; 6 Executive Office of the President organizations; 38 executive branch organizations associated with departments, agencies, or intelligence organizations; and 3 other organizations. These organizations are primarily located within 13 major departments and agencies mentioned in PDD 63.[24] Other departments and agencies, in addition to the 13 mentioned in PDD 63, are also involved in CIP activities. For example, the Department of Interior has cyber and

[22]GAO-01-822, September 20, 2001.

[23]GAO-02-474, July 15, 2002.

[24]These are the Departments of Commerce, Defense, Energy, Justice, Transportation, Health and Human Services, State, and Treasury; and the Environmental Protection Agency, the Federal Emergency Management Agency, the General Service Administration, and the National Science Foundation.

physical safeguard responsibilities associated with dams and the Department of Agriculture has responsibilities for food safety. Also, in addition to the over 50 organizations identified, agencies have cyber CIP activities specific to their department's systems, and other cyber security organizations receive federal funding. In addition, our review did not cover organizations with national physical CIP responsibilities like Transportation's Office of Pipeline Safety; Treasury's Bureau of Alcohol, Tobacco, and Firearms; and the Environmental Protection Agency's Chemical Emergency Preparedness and Prevention Office. Appendix I provides a high-level organization chart of the organizations we reviewed and more a detailed figure on component organizations' involvement, including a description of the type of CIP activities they perform. Appendix II displays in tabular format the entities and their activities.[25]

A clearly defined strategy is also essential for clarifying how CIP entities coordinate their activities with each other. Although most organizations in our review could identify relationships with other key cyber CIP entities, relationships among all organizations performing similar activities (e.g., policy development and analysis and warning) were not consistently established. For example, under PDD 63, the CIAO was set up to integrate the national CIP plan, coordinate a national education and awareness program, and coordinate legislative affairs. Nevertheless, of the organizations conducting policy development activities, only about one-half reported that they coordinated with the CIAO. Executive Order 13231, *Critical Infrastructure Protection in the Information Age,* acknowledged the need for additional coordination among organizations involved in cyber CIP by creating the President's Critical Infrastructure Protection Board to coordinate federal efforts and programs related to the protection of critical infrastructures. It is also important that any CIP-related efforts or proposals outside the scope of PDD 63 be coordinated with other CIP efforts. For example, we understand that EPA is considering a proposal that would require the 15,000 industrial facilities using hazardous chemicals to submit detailed vulnerability assessments.

Further, our report stated that an important aspect of this strategy will be the inclusion of additional potentially relevant critical infrastructure sectors or federal agencies that are not included in PDD 63. As mentioned previously, PDD 63 identifies 8 sector infrastructures with 13 lead agencies associated with the 8 sectors and 5 special functions. However, PDD 63 did not specifically address other possible critical sectors such as food supply, chemical manufacturing, and delivery services and their respective

[25]Appendix I displays the five general CIP activities according to a color-coded legend. Appendix II provides an alternative (table format) for black and white printing.

federal agency counterparts. Executive Order 13231 also did not change the sector infrastructures identified in PDD 63.

However, a few organizations stepped forward to address these gaps. For example, the Department of Agriculture, with responsibilities for food safety, recently established a Homeland Security Council, a departmentwide council with the mission of protecting the food supply and agricultural production. Also, a food ISAC has been recently formed by the Food Marketing Institute in conjunction with NIPC. Further, the chemical ISAC was established earlier this year.

We recommended in our July 2002 report, which was provided to the administration in May for comment, that when developing the strategy to guide federal CIP efforts, the Assistant to the President for National Security Affairs, the Assistant to the President for Homeland Security, and the Special Advisor to the President for Cyberspace Security ensure that, among other things, the strategy

- includes all relevant sectors and defines the key federal agencies' roles and responsibilities associated with each of the sectors, and
- defines the relationships among the key CIP organizations.

The newly issued national strategy for homeland security identifies 14 industry sectors, including the 8 identified in PDD 63. They are agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemical industry and hazardous materials, postal and shipping, and national monuments and icons.

National Strategy for Homeland Security Calls for the Development of Both Interim CIP Plans and a Comprehensive Plan

The national strategy for homeland security calls for interim cyber and physical infrastructure protection plans by September 2002, which are to be completed by the Office of Homeland Security and the President's Critical Infrastructure Protection Board. The strategy also states that the Department of Homeland Security would, building from the September plans, develop a comprehensive national infrastructure plan. The Department of Homeland Security strategy does not indicate a date when the comprehensive plan is to be completed.

According to the strategy, the national plan is to provide a methodology for identifying and prioritizing critical assets, systems, and functions, and for sharing protection responsibility with state and local government and

the private sector. The plan is to establish standards and benchmarks for infrastructure protection and provide a means to measure performance. The strategy also states that the Department of Homeland Security would unify the currently divided responsibilities for cyber and physical infrastructure. As we have previously recommended, this plan needs to clearly define the roles, responsibilities, and relationships among the many CIP organizations. Until a comprehensive and coordinated strategy is completed that identifies roles and responsibilities for all CIP efforts, our nation risks not having a consistent and appropriate structure to deal with the growing threat of computer-based attacks on its critical infrastructure.

Analysis and Warning Capabilities Need to Be Improved

Another key challenge is to develop more robust analysis and warning capabilities. NIPC was established in PDD 63 as "a national focal point" for gathering information on threats and facilitating the federal government's response to computer-based incidents. Specifically, the directive assigned NIPC the responsibility for providing comprehensive analyses on threats, vulnerabilities, and attacks; issuing timely warnings on threats and attacks; facilitating and coordinating the government's response to computer-based incidents; providing law enforcement investigation and response, monitoring reconstitution of minimum required capabilities after an infrastructure attack; and promoting outreach and information sharing. This responsibility requires obtaining and analyzing intelligence, law enforcement, and other information to identify patterns that may signal that an attack is underway or imminent. Similar activities are also called for in the President's proposal for the Information Analysis and Infrastructure Protection division.

In April 2001, we reported on NIPC's progress in developing national capabilities for analyzing threat and vulnerability data and issuing warnings, responding to attacks, among others.[26] Overall, we found that while progress in developing these capabilities was mixed, NIPC had initiated a variety of critical infrastructure protection efforts that had laid a foundation for future governmentwide efforts. In addition, NIPC had provided valuable support and coordination related to investigating and otherwise responding to attacks on computers. However, at the close of our review, the analytical capabilities that PDD 63 asserted are needed to protect the nation's critical infrastructures had not yet been achieved, and NIPC had developed only limited warning capabilities. Developing such capabilities is a formidable task that experts say will take an intense interagency effort.

[26]U.S. General Accounting Office, *Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities*, GAO-01-323 (Washington, D.C.: Apr. 25, 2001).

At the time of our review, NIPC had issued a variety of analytical products, most of which have been tactical analyses pertaining to individual incidents. In addition, it had issued a variety of publications, most of which were compilations of information previously reported by others with some NIPC analysis.

We reported that the use of strategic analysis to determine the potential broader implications of individual incidents had been limited. Such analysis looks beyond one specific incident to consider a broader set of incidents or implications that may indicate a potential threat of national importance. Identifying such threats assists in proactively managing risk, including evaluating the risks associated with possible future incidents and effectively mitigating the impact of such incidents.

We reported last year that three factors hindered NIPC's ability to develop strategic analytical capabilities:

- First, there was no generally accepted methodology for analyzing strategic cyber-based threats. For example, there was no standard terminology, no standard set of factors to consider, and no established thresholds for determining the sophistication of attack techniques. According to officials in the intelligence and national security community, developing such a methodology would require an intense interagency effort and dedication of resources.
- Second, NIPC had sustained prolonged leadership vacancies and did not have adequate staff expertise, in part because other federal agencies had not provided the originally anticipated number of detailees. For example, at the close of our review in February, the position of Chief of the Analysis and Warning Section, which was to be filled by the Central Intelligence Agency, had been vacant for about half of NIPC's 3-year existence. In addition, NIPC had been operating with only 13 of the 24 analysts that NIPC officials estimate are needed to develop analytical capabilities.
- Third, NIPC did not have industry-specific data on factors such as critical system components, known vulnerabilities, and interdependencies. Under PDD 63, such information is to be developed for each of eight industry segments by industry representatives and the designated federal lead agencies. However, at the close of our work, only three industry assessments had been partially completed, and none had been provided to NIPC. In September 2001, we reported that although outreach efforts had raised awareness and improved information sharing, substantive, comprehensive analysis of infrastructure sector interdependencies and vulnerabilities had been limited.

To provide a warning capability, NIPC had established a Watch and Warning Unit that monitors the Internet and other media 24 hours a day to identify reports of computer-based attacks. While some warnings were issued in time to avert damage, most of the warnings, especially those related to viruses, pertained to attacks underway. We reported that NIPC's ability to issue warnings promptly was impeded because of (1) a lack of a comprehensive governmentwide or nationwide framework for promptly obtaining and analyzing information on imminent attacks; (2) a shortage of skilled staff; (3) the need to ensure that NIPC does not raise undue alarm for insignificant incidents; and (4) the need to ensure that sensitive information is protected, especially when such information pertains to law enforcement investigations underway.

In addition, NIPC's own plans for further developing its analysis and warning capabilities were fragmented and incomplete. The relationships between the Center, the FBI, and the National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism at the National Security Council were unclear regarding who had direct authority for setting NIPC priorities and procedures and providing NIPC oversight. As a result, no specific priorities, milestones, or program performance measures existed to guide NIPC's actions or provide a basis for evaluating its progress.

In our report, we recognized that the administration was reviewing the government's infrastructure protection strategy and recommended that, as the administration proceeds, the Assistant to the President for National Security Affairs, in coordination with pertinent executive agencies,

- establish a capability for strategically analyzing computer-based threats, including developing related methodology, acquiring staff expertise, and obtaining infrastructure data;
- require development of a comprehensive data collection and analysis framework and ensure that national watch and warning operations for computer-based attacks are supported by sufficient staff and resources; and
- clearly define the role of NIPC in relation to other government and private-sector entities.

NIPC's director recently told us, in response to our report recommendations, that NIPC had developed a plan with goals and objectives to improve its analysis and warning capabilities and that NIPC has made considerable progress in this area. For example, the director told us that the analysis and warning section has created two additional teams to bolster its analytical capabilities: (1) the critical infrastructure

assessment team to focus efforts on learning about particular infrastructures and coordinating with respective infrastructure efforts and (2) the collection operations intelligence liaison team to coordinate with various entities within the intelligence community. The director added that NIPC (1) now holds a quarterly meeting with senior government leaders of entities that it regularly works with to better coordinate its analysis and warning capabilities; (2) has developed close working relationships with other CIP entities involved in analysis and warning activities, such as the Federal Computer Incident Response Center (FedCIRC), DOD's Joint Task Force for Computer Network Operations, the Carnegie Mellon's CERT® Coordination Center, and the intelligence and anti-virus communities; and (3) had developed and implemented procedures to more quickly share relevant CIP information, while separately continuing any related law enforcement investigation.

The director also stated that NIPC has received sustained leadership commitment from key entities, such as CIA and the National Security Agency, and that it continues to increase its staff primarily through reservists and contractors. The director acknowledged that our recommendations are not fully implemented and that despite the accomplishments to date, much more work remains to create the robust analysis and warning capabilities needed to adequately address cyberthreats.

Another challenge confronting the analysis and warning capabilities of our nation is that, historically, our national CIP attention and efforts have been focused on cyber threats. In April 2001, we reported that while PDD 63 covers both physical and computer-based threats, federal efforts to meet the directive's requirements have pertained primarily to computer-based threats, since this was an area that the leaders of the administration's CIP strategy viewed as needing attention. As we have stated earlier, swarming attacks, that employ concurrent cyber and physical attacks, are an emerging threat to the U.S. critical infrastructure.

The director told us that NIPC had begun to develop some capabilities for identifying physical CIP threats. For example, NIPC has developed thresholds with several ISACs for reporting physical incidents and has, since January 2002, issued several information bulletins concerning physical CIP threats. However, NIPC's director acknowledged that fully developing this capability will be a significant challenge.

Another critical issue in developing effective analysis and warning capabilities is to ensure that appropriate intelligence and other threat information, both cyber and physical, is received from the intelligence and

law enforcement communities. For example, considerable debate has ensued in recent weeks regarding the quality and timeliness of intelligence data shared between and among relevant intelligence, law enforcement, and other agencies. Also, with the President's proposed separation of NIPC from the FBI's law enforcement activities, including the Counterterrorism Division and NIPC field agents, it will be critical to establish mechanisms for continued communication to occur. Further, it will be important that the relationships between the law enforcement and intelligence communities and the proposed new Department of Homeland Security are effective and that appropriate information is exchanged on a timely basis.

In addition, according to NIPC's director, a significant challenge in developing a robust analysis and warning function is the development of the technology and human capital capacities to collect and analyze substantial amounts of information. Similarly, the Director of the FBI recently testified that implementing a more proactive approach to preventing terrorist acts and denying terrorist groups the ability to operate and raise funds requires a centralized and robust analytical capacity that does not currently exist in the FBI's Counterterrorism Division. He also stated that processing and exploiting information gathered domestically and abroad during the course of investigations requires an enhanced analytical and data mining capacity that is not presently available. Also, NIPC's director stated that multiagency staffing, similar to NIPC, is a critical success factor in establishing an effective analysis and warning function and that appropriate funding for such staff was important.

The national strategy for homeland security identifies intelligence and warning as one of six critical mission areas and calls for major initiatives to improve our nation's analysis and warning capabilities, including enhancing existing capabilities at the FBI and building new capabilities at the proposed Department of Homeland Security. The strategy also states that currently there is no government entity responsible for analyzing terrorist threats to the homeland, mapping these threats to our vulnerabilities, and taking protective action. Such responsibility would be given to the new Department of Homeland Security under the President's proposal. Further, the strategy states that the Department of Homeland Security is to have broad statutory authority to access intelligence information, as well as other information, relevant to the terrorist threat. In addition, the strategy indicates that the department would turn this information into useful warnings.

An important aspect of improving our nation's analysis and warning capabilities is having comprehensive vulnerability assessments. The

President's national strategy for homeland security also states that comprehensive vulnerability assessments of all of our nation's critical infrastructures are important from a planning perspective in that they enable authorities to evaluate the potential effects of an attack on a given sector and then invest accordingly to protect it. The strategy states that the U.S. government does not perform vulnerability assessments of all the nation's critical infrastructure. It further states that the new Department of Homeland Security would have the responsibility and capability of performing these comprehensive vulnerability assessments.

Government Faces Information Sharing Challenges

Information sharing is a key element in developing comprehensive and practical approaches to defending against cyber attacks, which could threaten the national welfare. Information on threats, vulnerabilities, and incidents experienced by others can help identify trends, better understand the risks faced, and determine what preventive measures should be implemented. However, as we testified in July 2000,[27] establishing the trusted relationships and information-sharing protocols necessary to support such coordination can be difficult.

Last October we reported on information sharing practices that could benefit CIP.[28] These practices include

- establishing trust relationships with a wide variety of federal and nonfederal entities that may be in a position to provide potentially useful information and advice on vulnerabilities and incidents;
- developing standards and agreements on how shared information will be used and protected;
- establishing effective and appropriately secure communications mechanisms; and
- taking steps to ensure that sensitive information is not inappropriately disseminated, which may require statutory changes.

In June of this year, we also reported on the information sharing barriers confronting homeland security, both within the federal government and with the private sector.[29]

[27]GAO/T-AIMD-00-268, July 26, 2000.

[28]U.S. General Accounting Office, *Information Sharing: Practices That Can Benefit Critical Infrastructure Protection*, GAO-02-24 (Washington, D.C.: Oct. 15, 2001).

[29]U.S. General Accounting Office, *National Preparedness: Integrating New and Existing Technology and Information Sharing Into an Effective Homeland Security Strategy*, GAO-02-811T (Washington, D.C.: June 7, 2002).

A number of activities have been undertaken to build relationships between the federal government and the private sector, such as InfraGard, the Partnership for Critical Infrastructure Security, efforts by the CIAO, and efforts by lead agencies to establish information sharing and analysis centers (ISACs). For example, the InfraGard Program, which provides the FBI and NIPC with a means of securely sharing information with individual companies, has expanded substantially. By early January 2001, 518 entities were InfraGard members—up from 277 members in October 2000. Members included representatives from private industry, other government agencies, state and local law enforcement, and the academic community. Currently, NIPC reports over 5,000 InfraGard members.

PDD 63 encouraged the voluntary creation of ISACs that could serve as the mechanism for gathering, analyzing, and appropriately sanitizing and disseminating information between the private sector and the federal government through NIPC. ISACs are critical since private-sector entities control over 80 percent of our nation's critical infrastructures. While PDD 63 encouraged the creation of ISACs, it left the actual design and functions of the ISACs, along with their relationship with NIPC, to be determined by the private sector in consultation with the federal government. PDD 63 did provide suggested activities which the ISACs could undertake, including:

- establishing baseline statistics and patterns on the various infrastructures;
- serving as a clearinghouse for information within and among the various sectors;
- providing a library for historical data for use by the private sector and government; and
- reporting private-sector incidents to NIPC.

In April 2001, we reported that NIPC and other government entities had not developed fully productive information-sharing relationships and that NIPC had undertaken a range of initiatives to foster information sharing relationships with ISACs, as well as government and international entities. We recommended that NIPC formalize relationships with ISACs and develop a plan to foster a two-way exchange of information between them.

In response to our recommendations, NIPC officials told us that a new ISAC development and support unit had been created, whose mission is to enhance private-sector cooperation and trust, resulting in a two-way sharing of information. NIPC now reports that over 10 ISACs have been established, including those for the chemical industry, surface transportation, electric power, telecommunications, information

technology, financial services, water supply, oil and gas, emergency fire services, food, and emergency law enforcement. Officials informed us that the center has signed information sharing agreements with most of these ISACs, including those representing telecommunications, information technology, water supply, food, emergency fire services, banking and finance, and chemical sectors. NIPC officials added that most of these agreements contained industry-specific cyber and physical incident reporting thresholds. Further, officials told us that NIPC has developed a program with the electric power ISAC whereby members transmit incident reports directly to the center. Table 1 lists both the PDD 63 sectors and additional sectors that the administration has acknowledged in its national strategy for homeland security, the lead federal agencies associated with each, ISACs that have been established according to NIPC, and ISACs that have entered into information sharing agreements with NIPC.

Table 1: Lead Agencies and ISAC Status by CIP Sector

Sectors identified by PDD 63 in 1998	Lead agency as designated in the national strategy for homeland security	ISAC established	Information sharing agreements with NIPC
Information and Telecommunication	Department of Homeland Security*		
Information technology		✓	✓
Telecommunications		✓	✓
Banking and finance	Department of the Treasury	✓	✓
Water	Environmental Protection Agency	✓	✓
Transportation	Department of Homeland Security*		
Air transportation			
Surface transportation		✓	
Waterborne commerce			
Emergency law enforcement**	Department of Homeland Security*	✓	✓
Emergency fire services,** continuity of government	Department of Homeland Security*		
Emergency fire services		✓	✓
*Continuity of government****			
Energy	Department of Energy		
Electric power		✓	✓
Oil and gas		✓	
Public health	Department of Health and Human Services		
New sectors identified in national strategy for homeland security			
Food	Department of Agriculture, Health and Human Services	✓	✓
Meat and poultry			
All other food products			
Agriculture	Department of Agriculture		
Chemical industry and hazardous materials	Environmental Protection Agency	✓	✓
Defense industrial base	Department of Defense		
Postal and shipping	Department of Homeland Security		
National monuments and icons	Department of the Interior		

*The lead agencies previously designated by PDD 63 were (from top to bottom) the Department of Commerce, Department of Transportation, Department of Justice/Federal Bureau of Investigations, and the Federal Emergency Management Agency.

**In the new national strategy for homeland security, emergency law enforcement and emergency fire services are included in an emergency services sector.

***In the new national strategy for homeland security, continuity of government, along with continuity of operations, is listed as a subcomponent under the government sector.

Despite progress establishing ISACs, more needs to be done. Each sector does not have a fully established ISAC, those that do have varied participation, and the amount of information being shared between the federal government and private sector organizations also varies.

Some in the private sector have expressed concerns about voluntarily sharing information with the government. For example, concerns have been raised that industry could potentially face antitrust violations for sharing information with other industry partners, have their information be subject to the Freedom of Information Act (FOIA), or face potential liability concerns for information shared in good faith. Many suggest that the government should model the Year 2000 Information and Readiness Disclosure Act, which provided limited exemptions and protections for the private sector in order to facilitate the sharing of information on Year 2000 readiness.

Other obstacles to information sharing, which were mentioned in recent congressional testimony, include difficulty obtaining security clearances for ISAC personnel and the reluctance to disclose corporate information. In recent congressional testimony, the Director of Information Technology for the North American Electric Reliability Council stated that the owners of critical infrastructures need access to more specific threat information and analysis from the public sector and that this may require either more security clearances or declassifying information.[30] The chief technology officer for BellSouth testified that an additional concern of the private sector in sharing information is the disclosure of sensitive corporate information to competitors. [31] Also, we previously reported that officials representing state and local governments, as well as the private sector, have concerns about funding homeland security.[32]

The private sector has also expressed its concerns about the value of information being provided by the government. For example, the President for the Partnership for Critical Infrastructure Security stated in congressional testimony earlier this month that information sharing between the government and private sector needs work, specifically, in

[30]Testimony of Lynn P. Constantini, Director, Information Technology, North American Electric Reliability Council, before the Subcommittee on Oversight and Investigations of the Committee on Energy and Commerce, U.S. House of Representatives, July 9, 2002.

[31] Statement of Bill Smith, Chief Technology Officer, BellSouth, before the Subcommittee on Oversight and Investigations of the Committee on Energy and Commerce, U.S. House of Representatives, July 9, 2002.

[32]U.S. General Accounting Office, *Homeland Security: Key Elements to Unify Efforts Are Underway, But Uncertainty Remains*, GAO-02-610 (Washington, D.C.: 2002).

the quality and timeliness of cyber security information coming from the government.

There will be continuing debate as to whether adequate protection is being provided to the private sector as these entities are encouraged to disclose and exchange information on both physical and cyber security problems and solutions that are essential to protecting our nation's critical infrastructures. The national strategy for homeland security, which outlines 12 major legislative initiatives, includes "enabling critical infrastructure information sharing." It states that the nation must meet this need by narrowly limiting public disclosure of information relevant to protecting our physical and cyber critical infrastructures in order to facilitate its voluntary submission. It further states that the Attorney General will convene a panel to propose any legal changes necessary to enable sharing of essential homeland security related information between the federal government and state and local governments. Actions have been taken by the Congress and the administration to strengthen information sharing. For example, the USA PATRIOT Act promotes information sharing among federal agencies, and numerous terrorism task forces have been established to coordinate investigations and improve communications among federal and local law enforcement.

Public policy tools will surely be discussed and reviewed as we look for additional means of improving information sharing. In the Comptroller General's testimony several weeks ago, he stated that intelligence and information sharing challenges highlight the need for strong partnerships with those outside the federal government and that the new department will need to design and manage tools of public policy (e.g., grants to nonfederal entities) to engage and work constructively with third parties.[33] We have previously testified on the choice and design of public policy tools that are available to governments.[34] These public policy tools include grants, regulations, tax incentives, and regional coordination and partnerships to motivate and mandate other levels of government or the private sector to address security concerns. As we have reported, the design of federal policy will play a vital role in determining the use and success of such tools in protecting the homeland. Some of these tools are already being used. For example, the Environmental Protection Agency recently announced that approximately 400 grants will be provided to assist large drinking water utilities in assessing their vulnerabilities. Consistent with the original intent of PDD 63, the national strategy for

[33]GAO-02-866T, June 25, 2002.

[34]U.S. General Accounting Office, *Combating Terrorism: Enhancing Partnerships Through a National Preparedness Strategy*, GAO 02-549T (Washington, D.C.: Mar. 28, 2002).

homeland security states that, in many cases, sufficient incentives exist in the private market to supply protection of America's critical infrastructures. However, the strategy also discusses the need to use available policy tools to raise the security of our critical infrastructures. For example, it mentions federal grants programs to assist state and local efforts, legislation to create incentives for the private sector, and regulation.

Information sharing within the government also remains a challenge. In April of last year, we reported that NIPC and other government entities had not developed fully productive information sharing and cooperative relationships. For example, federal agencies had not routinely reported incident information to NIPC, at least in part because guidance provided by the federal Chief Information Officers Council, which is chaired by the Office of Management and Budget, directs agencies to report such information to the General Services Administration's FedCIRC. Further, NIPC and DOD officials agreed that their information-sharing procedures needed improvement, noting that protocols for reciprocal exchanges of information had not been established. In addition, the expertise of the U.S. Secret Service regarding computer crime had not been integrated into NIPC efforts. According to NIPC's director, the relationship between NIPC and other government entities has significantly improved since our review, and that the quarterly meetings with senior government leaders have been instrumental in improving information sharing. In addition, officials from the Federal Computer Incident Response Center and the U.S. Secret Service in testimony have discussed the collaborative and cooperative relationships that now exist between their agencies and NIPC.

Pervasive Weaknesses in Federal Information Security Need to Be Addressed

At the federal level, cyber CIP activities are a component, perhaps the most critical, of a department or agency's overall information security program. Federal agencies have significant critical infrastructures that need effective information security to adequately protect them. However, since September 1996, we have reported that poor information security is a widespread federal problem with potentially devastating consequences.[35] Our analyses of information security at major federal agencies have shown that federal systems were not being adequately protected from computer-based threats, even though these systems process, store, and transmit enormous amounts of sensitive data and are indispensable to many federal agency operations. In addition, in both 1998 and in 2000, we analyzed audit results for 24 of the largest federal agencies and found that all 24 agencies

[35]U.S. General Accounting Office, *Information Security: Opportunities for Improved OMB Oversight of Agency Practices*, GAO/AIMD-96-110 (Washington, D.C.: Sept. 24, 1996).

had significant information security weaknesses.[36] As a result of these analyses, we have identified information security as a governmentwide high-risk issue in reports to the Congress since 1997—most recently in January 2001.[37] More current analyses of audit results, as well as of the agencies' own reviews of their information security programs, continue to show significant weaknesses that put critical federal operations and assets at risk.

Weaknesses Remain Pervasive

Our November 2001 analyses of audit results for 24 of the largest federal agencies showed that weaknesses continued to be reported in each of the 24 agencies.[38] These analyses considered GAO and inspector general (IG) reports published from July 2000 through September 2001, which included the first annual independent IG evaluations of agencies' information security programs required by government information security reform legislation (commonly referred to as "GISRA").[39]

Our analyses showed that the weaknesses reported for the 24 agencies covered all six major areas of general controls, that is, the policies, procedures, and technical controls that apply to all or a large segment of an entity's information systems and help ensure their proper operation. These six areas are (1) security program management, which provides the framework for ensuring that risks are understood and that effective controls are selected and properly implemented; (2) access controls, which ensure that only authorized individuals can read, alter, or delete data; (3) software development and change controls, which ensure that only authorized software programs are implemented; (4) segregation of

[36]U.S. General Accounting Office, *Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk*; GAO/AIMD-98-92 (Washington, D.C.: Sept. 23, 1998); *Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies*; GAO/AIMD-00-295 (Washington, D.C.: Sept. 6, 2000).

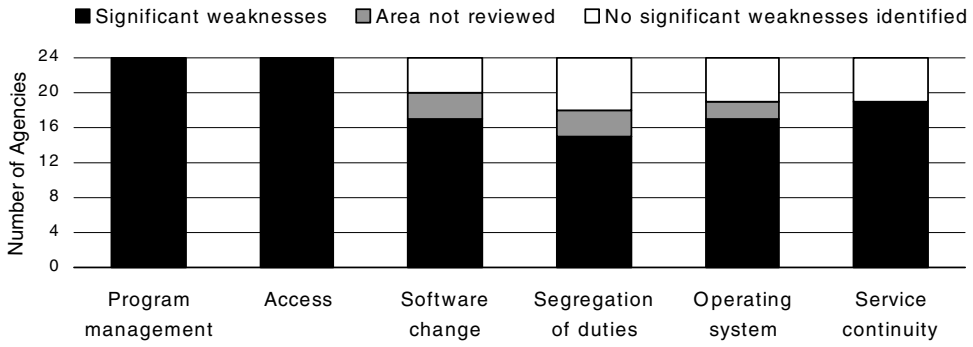
[37]U.S. General Accounting Office, *High-Risk Series: Information Management and Technology*; GAO/HR-97-9 (Washington, D.C.: Feb. 1, 1997); *High-Risk Series: An Update*; GAO/HR-99-1 (Washington, D.C.: Jan. 1999); *High-Risk Series: An Update*, GAO-01-263 (Washington, D.C.: Jan. 2001).

[38]U.S. General Accounting Office, *Computer Security: Improvements Needed to Reduce Risk to Critical Federal Operations and Assets*, GAO-02-231T (Washington, D.C.: Nov. 9, 2001).

[39]Title X, Subtitle G—Government Information Security Reform, Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001, P.L. 106-398, October 30, 2000. Congress enacted "GISRA" to supplement information security requirements established in the Computer Security Act of 1987, the Paperwork Reduction Act of 1995, and the Clinger-Cohen Act of 1996 and is consistent with existing information security guidance issued by OMB and the National Institute of Standards and Technology, as well as audit and best practice guidance issued by GAO. Most importantly, however, GISRA consolidates these separate requirements and guidance into an overall framework for managing information security and establishes new annual review, independent evaluation, and reporting requirements to help ensure agency implementation and both OMB and congressional oversight. Effective November 29, 2000, GISRA is in effect for 2 years after this date.

duties, which reduces the risk that one individual can independently perform inappropriate actions without detection; (5) operating systems controls, which protect sensitive programs that support multiple applications from tampering and misuse; and (6) service continuity, which ensures that computer-dependent operations experience no significant disruptions. Figure 3 illustrates the distribution of weaknesses for the six general control areas across the 24 agencies.

Figure 3: Information Security Weaknesses at 24 Major Agencies



Source: Audit reports issued July 2000 through September 2001.

As in 2000, our current analysis shows that weaknesses were most often identified for security program management and access controls. For security program management, we found weaknesses for all 24 agencies in 2001 as compared to 21 of the 24 agencies (88 percent) in 2000. Security program management, which is fundamental to the appropriate selection and effectiveness of the other categories of controls, covers a range of activities related to understanding information security risks; selecting and implementing controls commensurate with risk; and ensuring that controls, once implemented, continue to operate effectively. For access controls, we also found weaknesses for all 24 agencies in 2001—the same condition we found in 2000. Weak access controls for sensitive data and systems make it possible for an individual or group to inappropriately modify, destroy, or disclose sensitive data or computer programs for purposes such as personal gain or sabotage. In today's increasingly interconnected computing environment, poor access controls can expose an agency's information and operations to attacks from remote locations all over the world by individuals with only minimal computer and telecommunications resources and expertise. In 2001, we also found that 19 of the 24 agencies (79 percent) had weaknesses in service continuity controls (compared to 20 agencies or 83 percent in 2000). These controls are particularly important because they ensure that when unexpected

events occur, critical operations will continue without undue interruption and that crucial, sensitive data are protected. If service continuity controls are inadequate, an agency can lose the capability to process, retrieve, and protect electronically maintained information, which can significantly affect an agency's ability to accomplish its mission.

Our current analyses of information security at federal agencies also showed that the scope of audit work performed has continued to expand to more fully cover all six major areas of general controls at each agency. Not surprisingly, this has led to the identification of additional areas of weakness at some agencies. These increases in reported weaknesses do not necessarily mean that information security at federal agencies is getting worse. They more likely indicate that information security weaknesses are becoming more fully understood—an important step toward addressing the overall problem. Nevertheless, the results leave no doubt that serious, pervasive weaknesses persist. As auditors increase their proficiency and the body of audit evidence expands, it is probable that additional significant deficiencies will be identified.

Most of the audits represented in figure 3 were performed as part of financial statement audits. At some agencies with primarily financial missions, such as the Department of the Treasury and the Social Security Administration, these audits covered the bulk of mission-related operations. However, at agencies whose missions are primarily nonfinancial, such as the departments of Defense and Justice, the audits may provide a less complete picture of the agency's overall security posture because the audit objectives focused on the financial statements and did not include evaluations of individual systems supporting nonfinancial operations. In response to congressional interest, beginning in fiscal year 1999, we expanded our audit focus to cover a wider range of nonfinancial operations—a trend we expect to continue. Audit coverage for nonfinancial systems is also likely to increase as agencies review and evaluate their information security programs as required by GISRA.

Weaknesses Pose Substantial Risks for Federal Operations, Assets, and Confidentiality

To fully understand the significance of the weaknesses we identified, it is necessary to link them to the risks they present to federal operations and assets. Virtually all federal operations are supported by automated systems and electronic data, and agencies would find it difficult, if not impossible, to carry out their missions and account for their resources without these information assets. Hence, the degree of risk caused by security weaknesses is extremely high.

The weaknesses identified place a broad array of federal operations and assets at risk. For example,

- resources, such as federal payments and collections, could be lost or stolen;
- computer resources could be used for unauthorized purposes or to launch attacks on others;
- sensitive information, such as taxpayer data, social security records, medical records, and proprietary business information, could be inappropriately disclosed or browsed or copied for purposes of espionage or other types of crime;
- critical operations, such as those supporting national defense and emergency services, could be disrupted;
- data could be modified or destroyed for purposes of fraud or disruption; and
- agency missions could be undermined by embarrassing incidents that result in diminished confidence in their ability to conduct operations and fulfill their fiduciary responsibilities.

Examples from recent audit reports issued in 2001 illustrate the serious weaknesses found in the agencies that continue to place critical federal operations and assets at risk:

- In August, we reported that significant and pervasive weaknesses placed Commerce's systems at risk. Many of these systems are considered critical to national security, national economic security, and public health and safety. Nevertheless, we demonstrated that individuals, both within and outside of Commerce, could gain unauthorized access to Commerce systems and thereby read, copy, modify, and delete sensitive economic, financial, personnel, and confidential business data. Moreover, intruders could disrupt the operations of systems that are critical to the mission of the department.[40] Commerce's IG has also reported significant computer security weaknesses in several of the department's bureaus and, in February 2001, reported multiple material information security weaknesses affecting the department's ability to produce accurate data for financial statements.[41]

[40]U.S. General Accounting Office, *Information Security: Weaknesses Place Commerce Data and Operations at Serious Risk*; GAO-01-751 (Washington, D.C.: Aug. 13, 2001).

[41]Department of Commerce's Fiscal Year 2000 Consolidated Financial Statements, Inspector General Audit Report No. FSD-12849-1-0001.

- In July, we reported serious weaknesses in systems maintained by the Department of Interior's National Business Center, a facility processing more than $12 billion annually in payments, that place sensitive financial and personnel information at risk of unauthorized disclosure, critical operations at risk of disruption, and assets at risk of loss. While Interior has made progress in correcting previously identified weaknesses, the newly identified weaknesses impeded the center's ability to (1) prevent and detect unauthorized changes, (2) control electronic access to sensitive information, and (3) restrict physical access to sensitive computing areas.[42]

- In March, we reported that although DOD's Departmentwide Information Assurance Program made progress, it had not yet met its goals of integrating information assurance with mission-readiness criteria, enhancing information assurance capabilities and awareness of department personnel, improving monitoring and management of information assurance operations, and establishing a security management infrastructure. As a result, DOD was unable to accurately determine the status of information security across the department, the progress of its improvement efforts, or the effectiveness of its information security initiatives.[43]

- In February, the Department of Health and Human Services' IG again reported serious control weaknesses affecting the integrity, confidentiality, and availability of data maintained by the department.[44] Most significant were weaknesses associated with the department's Centers for Medicare and Medicaid Services (CMS), formerly known as the Health Care Financing Administration, which, during fiscal year 2000, was responsible for processing more than $200 billion in Medicare expenditures. CMS relies on extensive data processing operations at its central office to maintain administrative data (such as Medicare enrollment, eligibility, and paid claims data) and to process all payments for managed care. Significant weaknesses were also reported for the Food and Drug Administration and the department's Division of Financial Operations.

To correct reported weaknesses, several agencies took significant steps to redesign and strengthen their information security programs. For example, the Environmental Protection Agency has moved aggressively to reduce the exposure of its systems and data and to correct weaknesses we

[42]U.S. General Accounting Office, *Information Security: Weak Controls Place Interior's Financial and Other Data at Risk*; GAO-01-615 (Washington, D.C.: July 3, 2001).

[43]U.S. General Accounting Office, *Information Security: Progress and Challenges to an Effective Defense-wide Information Assurance Program*; GAO-01-307 (Washington, D.C.: Mar. 30, 2001).

[44]Report on the Financial Statement Audit of the Department of Health and Human Services for Fiscal Year 2000, A-17-00-00014, Feb. 26, 2001.

identified in February 2000.[45] While we have not tested their effectiveness, these actions show that the agency is taking a comprehensive and systematic approach that should help ensure that its efforts are effective.

Agencies' GISRA Results Also Highlight Weaknesses

As required by GISRA, agencies reviewed their information security programs, reported the results of these reviews and the IGs' independent evaluations to OMB, and developed plans to correct identified weaknesses. These reviews and evaluations showed that agencies have not established information security programs consistent with GISRA requirements and that significant weaknesses exist. Although agency actions are now underway to strengthen information security and implement these requirements, significant improvement will require sustained management attention and OMB and congressional oversight.

In its fiscal year 2001 report to the Congress on GISRA, OMB notes that although examples of good security exist in many agencies, and others are working very hard to improve their performance, many agencies have significant deficiencies in every important area of security.[46] In particular, the report highlights six common security weaknesses: (1) a lack of senior management attention to information security; (2) inadequate accountability for job and program performance related to information technology security; (3) limited security training for general users, information technology professionals, and security professionals; (4) inadequate integration of security into the capital planning and investment control process; (5) poor security for contractor-provided services; and (6) limited capability to detect, report, and share information on vulnerabilities or to detect intrusions, suspected intrusions, or virus infections.

In general, our analyses of the results of agencies' GISRA reviews and evaluations also showed that agencies are making progress in addressing information security, but that none of the agencies had fully implemented the information security requirements of GISRA and all continue to have significant weaknesses. In particular, our review of 24 of the largest federal agencies showed that agencies had not fully implemented requirements to

- conduct risk assessments for all their systems;

[45] U.S. General Accounting Office, *Information Security: Fundamental Weaknesses Place EPA Data and Operations at Risk*; GAO/AIMD-00-215 (Washington, D.C.: July 6, 2000).

[46] Office of Management and Budget, *FY 2001 Report to Congress on Federal Government Information Security Reform* (Feb. 2002).

- establish information security policies and procedures that are commensurate with risk and that comprehensively address the other reform provisions;
- provide adequate computer security training to their employees including contractor staff;
- test and evaluate controls as part of their management assessments;
- implement documented incident handling procedures agencywide;
- identify and prioritize their critical operations and assets, and determine the priority for restoring these assets should a disruption in critical operations occur; or
- have a process to ensure the security of services provided by a contractor or another agency.

H.R. 3844 would permanently authorize and strengthen the information security program, evaluation, and reporting requirements established by GISRA, which is to expire on November 29, 2002. As demonstrated by its first-year implementation, GISRA proved to be a significant step in improving federal agencies' information security programs and addressing their serious, pervasive information security weaknesses. Agencies have noted benefits from GISRA, such as increased management attention to and accountability for information security. In addition, the administration has taken important actions to address information security into the President's Management Agenda Scorecard. We believe that continued authorization of such important information security legislation is essential to sustaining agency efforts to identify and correct significant weaknesses. Further, this authorization would reinforce the federal government's commitment to establishing information security as an integral part of its operations and help ensure that the administration and the Congress continue to receive the information they need to effectively manage and oversee federal information security.

Improvement Efforts are Underway, But Challenges to Federal Information Security Remain

Information security improvement efforts have been undertaken in the past few years both at an agency and governmentwide level. However, given recent events and reports that critical operations and assets continue to be highly vulnerable to computer-based attacks, the government still faces a challenge in ensuring that risks from cyber threats are appropriately addressed. Accordingly, it is important that federal

information security efforts be guided by a comprehensive strategy for improvement.

First, it is important that the federal strategy delineate the roles and responsibilities of the numerous entities involved in federal information security. This strategy should also consider other organizations with information security responsibilities, including OMB, which oversees and coordinates federal agency security, and interagency bodies like the CIO Council, which are attempting to coordinate agency initiatives. It should also describe how the activities of these many organizations interrelate, who should be held accountable for their success or failure, and whether they will effectively and efficiently support national goals.

Second, more specific guidance to agencies on the controls that they need to implement could help ensure adequate protection. Currently, agencies have wide discretion in deciding what computer security controls to implement and the level of rigor with which to enforce these controls. In theory, this discretion is appropriate since, as OMB and NIST guidance states, the level of protection that agencies provide should be commensurate with the risk to agency operations and assets. In essence, one set of specific controls will not be appropriate for all types of systems and data. Nevertheless, our studies of best practices at leading organizations have shown that more specific guidance is important.[47] In particular, specific mandatory standards for varying risk levels can clarify expectations for information protection, including audit criteria; provide a standard framework for assessing information security risk; help ensure that shared data are appropriately protected; and reduce demands for limited resources to independently develop security controls. Implementing such standards for federal agencies would require developing a single set of information classification categories for use by all agencies to define the criticality and sensitivity of the various types of information they maintain. It would also necessitate establishing minimum mandatory requirements for protecting information in each classification category.

Third, ensuring effective implementation of agency information security and CIP plans will require active monitoring by the agencies to determine if milestones are being met and testing to determine if policies and controls are operating as intended. Routine periodic audits, such as those required by GISRA, would allow for more meaningful performance measurement. In addition, the annual evaluation, reporting, and

[47]U.S. General Accounting Office, *Information Security Management: Learning from Leading Organizations*, GAO/AIMD-98-68 (Washington, D.C.: May 1998).

monitoring process established through these provisions is an important mechanism, previously missing, to hold agencies accountable for implementing effective security and to manage the problem from a governmentwide perspective. Moreover, with GISRA expiring on November 29, 2002, we believe that continued authorization of information security legislation is essential to improving federal information security.

The implementation of GISRA has also resulted in important actions by the administration, which if properly implemented, should continue to improve information security in the federal government. For example, OMB has issued guidance that information technology investments will not be funded unless security is incorporated into and funded as part of each investment. The administration also has plans to

- direct all large agencies to undertake a review to identify and prioritize critical assets within the agencies and their interrelationships with other agencies and the private sector, as well as a cross-government review to ensure that all critical government processes and assets have been identified;
- integrate security into the President's Management Agenda Scorecard;
- develop workable measures of performance;
- develop e-training on mandatory topics, including security; and
- explore methods to disseminate vulnerability patches to agencies more effectively.

Fourth, the Congress and the executive branch can use audit results to monitor agency performance and take whatever action is deemed advisable to remedy identified problems. Such oversight is essential for holding agencies accountable for their performance, as was demonstrated by OMB and congressional efforts to oversee the Year 2000 computer challenge.

Fifth, agencies must have the technical expertise they need to select, implement, and maintain controls that protect their information systems. Similarly, the federal government must maximize the value of its technical staff by sharing expertise and information. Highlighted during the Year 2000 challenge, the availability of adequate technical and audit expertise is a continuing concern to agencies.

Sixth, agencies can allocate resources sufficient to support their information security and infrastructure protection activities. Funding for security is already embedded to some extent in agency budgets for

computer system development efforts and routine network and system management and maintenance. However, some additional amounts are likely to be needed to address specific weaknesses and new tasks. OMB and congressional oversight of future spending on information security will be important to ensuring that agencies are not using the funds they receive to continue ad hoc, piecemeal security fixes that are not supported by a strong agency risk management process.

Seventh, expanded research is needed in the area of information systems protection. While a number of research efforts are underway, experts have noted that more is needed to achieve significant advances. As stated by the director of the CERT® Coordination Center in congressional testimony last September, "It is essential to seek fundamental technological solutions and to seek proactive, preventive approaches, not just reactive, curative approaches."[48] In addition, in its December 2001 third annual report, the Gilmore Commission recommended that the Office of Homeland Security develop and implement a comprehensive plan for research, development, test, and evaluation to enhance cyber security.[49]

In conclusion, prior GAO work has identified and made recommendations concerning several CIP challenges that need to be addressed. These include

- completing a comprehensive and coordinated CIP strategy that includes both cyber and physical aspects, defines the roles and responsibilities of the many CIP organizations, and establishes objectives, timeframes, and performance measures;
- improving analysis and warning capabilities to address the potential disruption of both cyber and physical threats and vulnerabilities;
- improving information sharing both within the federal government and between the federal government and the private sector and state and local governments; and
- addressing pervasive weaknesses in federal information security.

Although the President's national strategy for homeland security discusses many of these challenges, much work remains to effectively address them.

[48]Testimony of Richard D. Pethia, Director, CERT® Centers, Software Engineering Institute, Carnegie Mellon University, before the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, U.S. House Committee on Government Reform, September 26, 2001.

[49]*Third Annual Report to the President and Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction* (Dec. 15, 2001).

The CIP plans that are expected to be released in September and the comprehensive CIP plan to be completed at a later date are important steps in protecting our critical infrastructures. However, even more critical to protecting our country against terrorism is successfully implementing these plans.

Mr. Chairman, this concludes my written testimony. I would be pleased to answer any questions that you or other members of the Subcommittee may have at this time.

If you should have any questions about this testimony, please contact me at (202) 512-3317. I can also be reached by e-mail at daceyr@gao.gov.

Appendix I
Organizations Involved in National or Multiagency CIP Activities

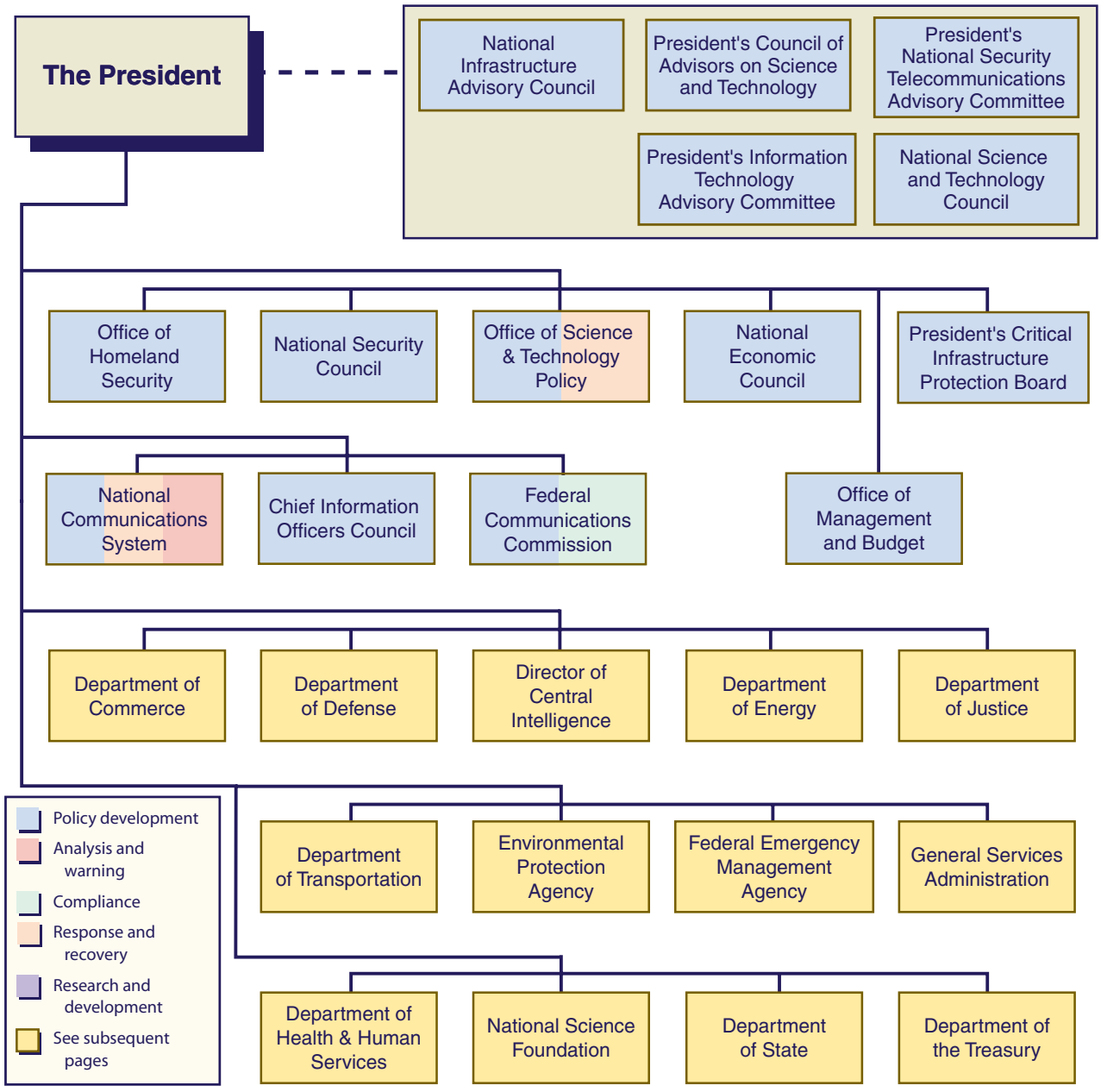
Although each organization involved in our review of national or multiagency cyber critical infrastructure protection (CIP) efforts described a wide range of cyber CIP related activities, collectively they described activities related to the following five categories:[50]

- policy development, including advising on policy issues, coordinating and planning CIP activities, issuing standards and best practices, providing input to the national CIP plan, developing education and outreach programs with governmental and private sector organizations, and coordinating internationally;
- analysis and warning, including conducting vulnerability analyses, gathering intelligence information, coordinating and directing activities to detect computer-based attacks, disseminating information to alert organizations of potential and actual infrastructure attacks, and facilitating the sharing of security related information;
- compliance, including overseeing implementation of cyber CIP programs, ensuring that policy is adhered to and remedial plans are developed, and investigating cyberattacks on critical infrastructures;
- response and recovery, including reconstituting minimum required capabilities, isolating and minimizing damage, and coordinating the necessary actions to restore functionality; and
- research and development, including coordinating federally sponsored research and development in support of infrastructure protection.

Figure 4 displays a high-level overview of the organizational placement of the 5 advisory committees; 6 Executive Office of the President organizations; 13 executive branch departments and agencies; and several other organizations involved in national or multiagency cyber CIP efforts. For departments and agencies, figure 5 provides further detail on component organizations' involvement, but does not illustrate the internal relationships within each agency. For all figures, organizations' cyber CIP-related activities are identified in one or more of the five general categories discussed above.

[50]GAO-02-474, July 15, 2002.

Figure 4: Overview of National or Multiagency Federal Cyber CIP Organizations



Note: Major agencies or departments are highlighted in yellow here and on the following pages. The organizations are color-coded to correspond to one or more of the five general activities related to cyber CIP (see legend on figures).

Figure 5: Components of Executive Departments or Agencies and Their Primary Activities Related to Cyber CIP (as Indicated by the Color-Coded Legend Below)

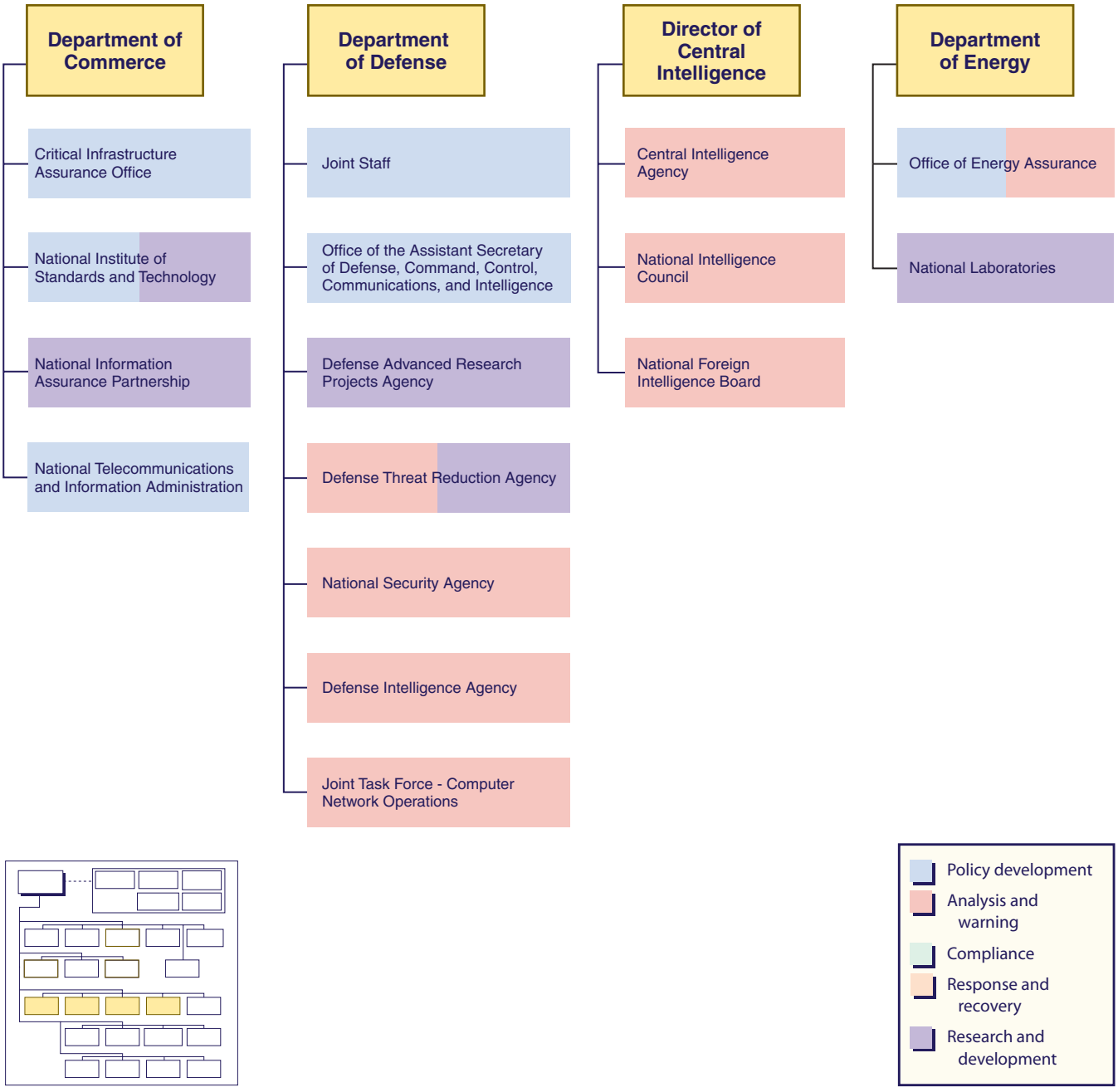


Figure 5 (cont'd): Components of Executive Departments or Agencies and Their Primary Activities Related to Cyber CIP (as Indicated by the Color-Coded Legend Below)

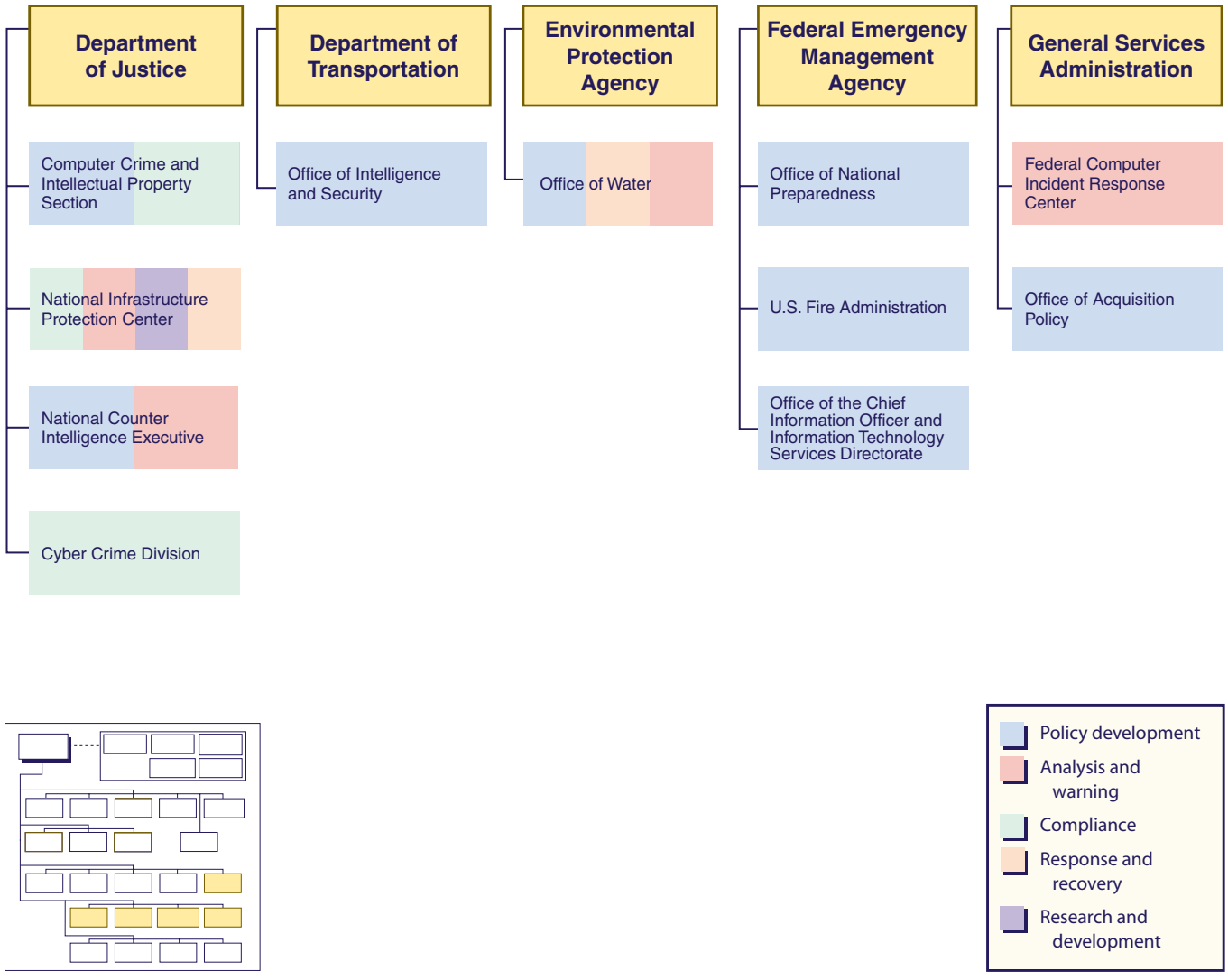
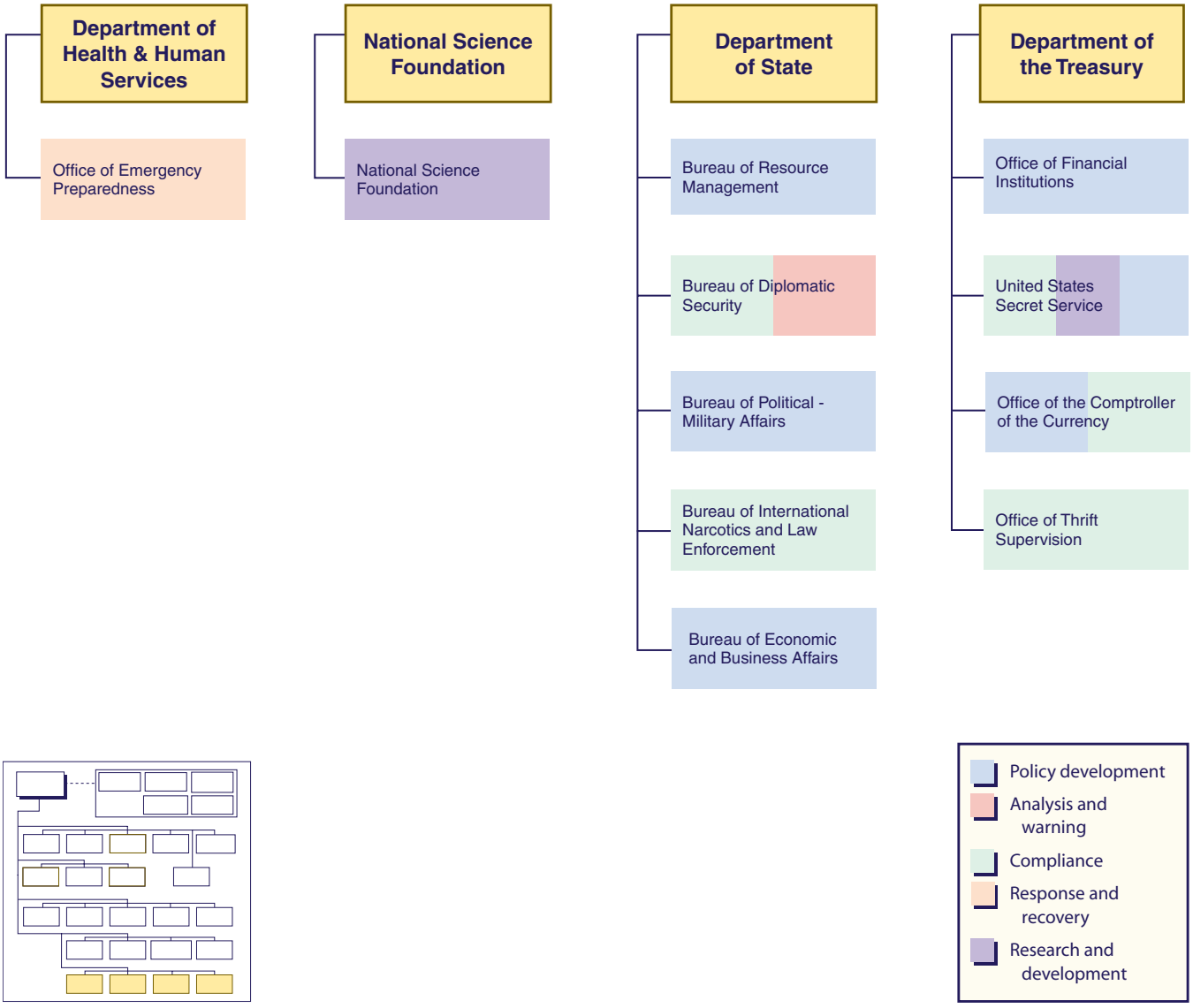


Figure 5 (cont'd): Components of Executive Departments or Agencies and Their Primary Activities Related to Cyber CIP (as Indicated by the Color-Coded Legend Below)



Appendix II
Components of Executive Departments or Agencies and their Primary Activities Related to Cyber CIP

Table 2: Executive Department or Agency Components and their Primary Activities Related to Cyber CIP

Organization	Policy development	Analysis & warning	Compliance	Response & recovery	Research & development
Federal Advisory Committees					
National Infrastructure Advisory Council	√				
President's Council of Advisors on Science and Technology	√				
President's National Security Telecommunications Advisory Committee	√				
President's Information Technology Advisory Committee					
National Science and Technology Council	√				
Executive Office of the President					
Office of Homeland Security	√				
National Security Council	√				
Office of Science and Technology Policy	√			√	
National Communications System	√	√		√	
National Economic Council	√				
Office of Management and Budget	√				
President's Critical Infrastructure Protection Board	√				
Chief Information Officers Council	√				
Federal Communications Commission	√		√		
U.S. Department of Commerce					
Critical Infrastructure Assurance Office	√				
National Institute of Standards and Technology	√				√
National Information Assurance Partnership					√

Organization	Policy development	Analysis & warning	Compliance	Response & recovery	Research & development
National Telecommunications and Information Administration	√				
U.S. Department of Defense					
Joint Staff	√				
Office of the Assistant Secretary of Defense, Command, Control, Communications, and Intelligence	√				
Defense Advanced Research Projects Agency					√
Defense Threat Reduction Agency		√			√
National Security Agency		√			
Defense Intelligence Agency		√			
Joint Task Force - Computer Network Operations		√			
Director of Central Intelligence					
Central Intelligence Agency		√			
National Intelligence Council		√			
National Foreign Intelligence Board		√			
U.S. Department of Energy					
Office of Energy Assurance	√	√			
National Laboratories					√
U.S. Department of Justice					
Computer Crime and Intellectual Property Section	√		√		
National Infrastructure Protection Center		√	√	√	√
National Counter Intelligence Executive	√	√			
Cyber Crime Division			√		
U.S. Department of Transportation					
Office of Intelligence and Security	√				

Organization	Policy development	Analysis & warning	Compliance	Response & recovery	Research & development
Environmental Protection Agency					
Office of Water	√	√		√	
Federal Emergency Management Agency					
Office of National Preparedness	√				
United States Fire Administration	√				
Office of the Chief Information Officer and Information Technology Services Directorate	√				
U.S. General Services Administration					
Federal Computer Incident Response Center		√			
Office of Acquisition Policy	√				
Department of Health and Human Services					
Office of Emergency Preparedness				√	
National Science Foundation					√
U.S. Department of State					
Bureau of Resource Management	√				
Bureau of Diplomatic Security		√	√		
Bureau of Political-Military Affairs	√				
Bureau of International Narcotics and Law Enforcement			√		
Bureau of Economic and Business Affairs	√				
U.S. Department of Treasury					
Office of Financial Institutions	√				
United States Secret Service	√		√		√
Office of the Comptroller of the Currency	√		√		
Office of Thrift Supervision			√		

Appendix III
Related GAO Products Issued Since Fiscal Year 1996

Critical Infrastructure Protection: Federal Efforts Require a More Coordinated and Comprehensive Approach for Protecting Information Systems. GAO-02-474. Washington, D.C.: July 15, 2002.

FDIC Information Security: Improvements Made But Weaknesses Remain. GAO-02-689. Washington, D.C.: July 15, 2002.

Critical Infrastructure Protection: Significant Homeland Security Challenges Need to Be Addressed. GAO-02-918T. Washington, D.C.: July 9, 2002.

Information Security: Corps of Engineers Making Improvements, but Weaknesses Continue. GAO-02-589. Washington, D.C.: June 10, 2002.

National Preparedness: Integrating New and Existing Technology and Information Sharing into an Effective Homeland Security Strategy. GAO-02-811T. Washington, D.C.: June 7, 2002.

Information Security: Comments on the Proposed Federal Information Security Management Act of 2002. GAO-02-677T. Washington, D.C.: May 2, 2002.

Information Security: Additional Actions Needed to Fully Implement Reform Legislation. GAO-02-407. Washington, D.C.: May 2, 2002.

Information Security: Subcommittee Post-Hearing Questions Concerning the Additional Actions Needed to Implement Reform Legislation. GAO-02-649R. Washington, D.C.: April 16, 2002.

Information Security: Additional Actions Needed to Implement Reform Legislation. GAO-02-470T. Washington, D.C.: March 6, 2002.

Financial Management Service: Significant Weaknesses in Computer Controls Continue. GAO-02-317. Washington, D.C.: January 31, 2002.

Federal Reserve Banks: Areas for Improvement in Computer Controls. GAO-02-266R. Washington, D.C.: December 10, 2001.

Computer Security: Improvements Needed to Reduce Risk to Critical Federal Operations and Assets. GAO-02-231T. Washington, D.C.: November 9, 2001.

Information Sharing: Practices That Can Benefit Critical Infrastructure Protection. GAO-02-24. Washington, D.C.: October 15, 2001.

Critical Infrastructure Protection: Significant Challenges in Safeguarding Government and Privately-Controlled Systems from Computer-Based Attacks. GAO-01-1168T. Washington, D.C.: September 26, 2001.

Combating Terrorism: Selected Challenges and Related Recommendations. GAO-01-822. Washington, D.C.: September 20, 2001.

Bureau of the Public Debt: Areas for Improvement in Computer Controls. GAO-01-1131R. Washington, D.C.: September 13, 2001.

Critical Infrastructure Protection: Significant Challenges in Protecting Federal Systems and Developing Analysis and Warning Capabilities. GAO-01-1132T. Washington, D.C.: September 12, 2001.

Education Information Security: Improvements Made But Control Weaknesses Remain. GAO-01-1067. Washington, D.C.: September 12, 2001.

Information Security: Code Red, Code Red II, and SirCam Attacks Highlight Need for Proactive Measures. GAO-01-1073T. Washington, D.C.: August 29, 2001.

Nuclear Security: DOE Needs to Improve Control Over Classified Information. GAO-01-806. Washington, D.C.: August 24, 2001.

Information Security: Weaknesses Place Commerce Data and Operations at Serious Risk. GAO-01-751. Washington, D.C.: August 13, 2001.

Information Security: Weaknesses Place Commerce Data and Operations at Serious Risk. GAO-01-1004T. Washington, D.C.: August 3, 2001.

Information Systems: Opportunities Exist to Strengthen SEC's Oversight of Capacity and Security. GAO-01-863. Washington, D.C.: July 25, 2001.

Critical Infrastructure Protection: Significant Challenges in Developing Analysis, Warning, and Response Capabilities. GAO-01-1005T. Washington, D.C.: July 25, 2001.

Information Security: Weak Controls Place Interior's Financial and Other Data at Risk. GAO-01-615. Washington, D.C.: July 3, 2001.

Critical Infrastructure Protection: NIPC Faces Significant Challenges in Developing Analysis, Warning, and Response Capabilities. GAO-01-769T. Washington, D.C.: May 22, 2001.

Computer-Based Patient Records: Better Planning and Oversight by VA, DOD, and HHS Would Enhance Health Data Sharing. GAO-01-459. Washington, D.C.: April 30, 2001.

Internet Privacy: Implementation of Federal Guidance for Agency Use of "Cookies." GAO-01-424. Washington, D.C.: April 27, 2001.

Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities. GAO-01-323. Washington, D.C.: April 25, 2001.

Computer Security: Weaknesses Continue To Place Critical Federal Operations And Assets At Risk. GAO-01-600T. Washington, D.C.: April 5, 2001.

VA Information Technology: Important Initiatives Begun, Yet Serious Vulnerabilities Persist. GAO-01-550T. Washington, D.C.: April 4, 2001.

Internal Revenue Service: 2001 Tax Filing Season, Systems Modernization, and Security of Electronic Filing. GAO-01-595T. Washington, D.C.: April 3, 2001.

Internal Revenue Service: Progress Continues But Serious Management Challenges Remain. GAO-01-562T. Washington, D.C.: April 2, 2001.

Information Security: Safeguarding of Data in Excessed Department of Energy Computers . GAO-01-469. Washington, D.C.: March 29, 2001.

U.S. Government Financial Statements: FY 2000 Reporting Underscores the Need to Accelerate Federal Financial Management Reform. GAO-01-570T. Washington, D.C.: March 30,2001.

Information Security: Challenges to Improving DOD's Incident Response Capabilities. GAO-01-341. Washington, D.C.: March 29, 2001.

Information Security: Progress and Challenges to an Effective Defense-Wide Information Assurance Program. GAO-01-307. Washington, D.C.: March 30, 2001.

Information Security: IRS Electronic Filing Systems. GAO-01-306. Washington, D.C.: February 16, 2001.

Information Security: Advances and Remaining Challenges to Adoption of Public Key Infrastructure Technology. GAO-01-277. Washington, D.C.: February 26, 2001.

Information Security: Weak Controls Place DC Highway Trust Fund and Other Data at Risk. GAO-01-155. Washington, D.C.: January 31, 2001.

High Risk Series: An Update. GAO-01-263. Washington, D.C.: January 2001.

FAA Computer Security: Recommendations to Address Continuing Weaknesses. GAO-01-171. Washington, D.C.: December 6, 2000.

Financial Management: Significant Weaknesses in Corps of Engineers' Computer Controls. GAO-01-89. Washington, D.C.: October 11, 2000.

FAA Computer Security: Actions Needed to Address Critical Weaknesses That Jeopardize Aviation Operations. GAO/T-AIMD-00-330. Washington, D.C.: September 27, 2000.

Financial Management Service: Significant Weaknesses in Computer Controls. GAO/AIMD-00-305. Washington, D.C.: September 26, 2000.

VA Information Technology: Progress Continues Although Vulnerabilities Remain. GAO/T-AIMD-00-321. Washington, D.C.: September 21, 2000.

Electronic Government: Government Paperwork Elimination Act Presents Challenges for Agencies. GAO/AIMD-00-282. Washington, D.C.: September 15, 2000.

Year 2000 Computer Challenge: Lessons Learned Can Be Applied to Other Management Challenges. GAO/AIMD-00-290. Washington, D.C.: September 12, 2000.

VA Information Systems: Computer Security Weaknesses Persist at the Veterans Health Administration. GAO/AIMD-00-232. Washington, D.C.: September 8, 2000.

Computer Security: Critical Federal Operations and Assets Remain at Risk. GAO/T-AIMD-00-314. Washington, D.C.: September 11, 2000.

Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies. GAO/AIMD-00-295. Washington, D.C.: September 6, 2000.

FAA Computer Security: Concerns Remain Due to Personnel and Other Continuing Weaknesses. GAO/AIMD-00-252. Washington, D.C.: August 16, 2000.

Information Security: USDA Needs to Implement Its Departmentwide Information Security Plan. GAO/AIMD-00-217. Washington, D.C.: August 10, 2000.

Information Technology: Selected Agencies' Use of Commercial Off-the-Shelf Software for Human Resources Functions. GAO/AIMD-00-270. Washington, D.C.: July 31, 2000.

Bureau of the Public Debt: Areas for Improvement in Computer Controls. GAO/AIMD-00-269. Washington, D.C.: August 9, 2000.

Critical Infrastructure Protection: Challenges to Building a Comprehensive Strategy for Information Sharing and Coordination. GAO/T-AIMD-00-268. Washington, D.C.: July 26, 2000.

Electronic Signature: Sanction of the Department of State's System. GAO/AIMD-00-227R. Washington, D.C.: July 10, 2000.

Information Security: Fundamental Weaknesses Place EPA Data and Operations at Risk. GAO/AIMD-00-215. Washington, D.C.: July 6, 2000.

Nuclear Security: Information on DOE's Requirements for Protecting and Controlling Classified Documents. GAO/T-RCED-00-247. Washington, D.C.: July 11, 2000.

Federal Reserve Banks: Areas for Improvement in Computer Controls. GAO/AIMD-00-218. Washington, D.C.: July 7, 2000.

Critical Infrastructure Protection: Comments on the Proposed Cyber Security Information Act of 2000. GAO/T-AIMD-00-229. Washington, D.C.: June 22, 2000.

Computer Security: FAA Is Addressing Personnel Weaknesses, but Further Action Is Required. GAO/AIMD-00-169. Washington, D.C.: May 31, 2000.

Critical Infrastructure Protection: "ILOVEYOU" Computer Virus Highlights Need for Improved Alert and Coordination Capabilities. GAO/T-AIMD-00-181. Washington, D.C.: May 18, 2000.

Information Security: "ILOVEYOU" Computer Virus Emphasizes Critical Need for Agency and Governmentwide Improvements. GAO/T-AIMD-00-171. Washington, D.C.: May 10, 2000.

Information Security: Controls Over Software Changes at Federal Agencies. GAO/AIMD-00-151R. Washington, D.C.: May 4, 2000.

VA Systems Security: Information System Controls at the VA Maryland Health Care System. GAO/AIMD-00-117R. Washington, D.C.: April 19, 2000.

Federal Information Security: Action Needed to Address Widespread Weaknesses. GAO/T-AIMD-00-135. Washington, D.C.: March 29, 2000.

Export Controls: National Security Risks and Revisions to Controls on Computer Systems. GAO/T-NSIAD-00-139. Washington, D.C.: March 23, 2000.

Financial Management: USDA Faces Major Financial Management Challenges. GAO/T-AIMD-00-115. Washington, D.C.: March 21, 2000.

Information Security: Comments on Proposed Government Information Security Act of 1999. GAO/T-AIMD-00-107. Washington, D.C.: March 2, 2000.

Information Security: Fundamental Weaknesses Place EPA Data and Operations at Risk. GAO/T-AIMD-00-97. Washington, D.C.: February 17, 2000.

Computer Security: Reported Appropriations and Obligations for Four Major Initiatives. GAO/AIMD-00-92R. Washington, D.C.: February 28, 2000.

Critical Infrastructure Protection: National Plan for Information Systems Protection. GAO/AIMD-00-90R. Washington, D.C.: February 11, 2000.

Critical Infrastructure Protection: Comments on the National Plan for Information Systems Protection. GAO/T-AIMD-00-72. Washington, D.C.: February 01, 2000.

Computer Security: FAA Needs to Improve Controls Over Use of Foreign Nationals to Remediate and Review Software. GAO/AIMD-00-55. Washington, D.C.: December 23, 1999.

Information Security: Responses to Posthearing Questions. GAO/AIMD-00-46R. Washington, D.C.: November 30, 1999. Sen. Judiciary Committee.

Information Security Risk Assessment: Practice of Leading Organizations (A supplement to GAO's May 1998 Executive Guide on Information Security Management.) GAO/AIMD-00-33. Washington, D.C.: November 1999.

Information Security: Weaknesses at 22 Agencies. GAO/AIMD-00-32R. Washington, D.C.: November 10, 1999.

Information Security: SSA's Computer Intrusion Detection Capabilities. GAO/AIMD-00-16R. Washington, D.C.: October 27, 1999.

Critical Infrastructure Protection: Fundamental Improvements Needed to Assure Security of Federal Operations. GAO/T-AIMD-00-7. Washington, D.C.: October 6, 1999.

Financial Management Service: Significant Weaknesses in Computer Controls. GAO/AIMD-00-4, Oct. 4, 1999.

Information Systems: The Status of Computer Security at the Department of Veterans Affairs. GAO/AIMD-00-5. Washington, D.C.: October 4, 1999.

Critical Infrastructure Protection: Comprehensive Strategy Can Draw on Year 2000 Experiences. GAO/AIMD-00-1. Washington, D.C.: October 1, 1999.

Information Security: The Proposed Computer Security Enhancement Act of 1999. GAO/T-AIMD-99-302. Washington, D.C.: September 30, 1999.

Federal Reserve Banks: Areas for Improvement in Computer Controls. GAO/AIMD-99-280. Washington, D.C.: September 15, 1999.

Information Security: NRC's Computer Intrusion Detection Capabilities. GAO/AIMD-99-273R. Washington, D.C.: August 27, 1999.

DOD Information Security: Serious Weaknesses Continue to Place Defense Operations at Risk. GAO/AIMD-99-107. Washington, D.C.: August 26, 1999.

Battlefield Automation: Opportunities to Improve the Army's Information Protection Effort. GAO/NSIAD-99-166. Washington, D.C.: August 11, 1999.

Information Security: Answers to Posthearing Questions. GAO/AIMD-99-272R. Washington, D.C.: August 9, 1999.

Bureau of the Public Debt: Areas for Improvement in Computer Controls. GAO/AIMD-99-242. Washington, D.C.: August 6, 1999.

USDA Information Security: Weaknesses at National Finance Center Increase Risk of Fraud, Misuse, and Improper Disclosure. GAO/AIMD-99-227. Washington, D.C.: July 30, 1999.

Medicare: Improvements Needed to Enhance Protection of Confidential Health Information. HEHS-99-140. Washington, D.C.: July 20, 1999.

Medicare: HCFA Needs to Better Protect Beneficiaries' Confidential Health Information. GAO/T-HEHS-99-172. Washington, D.C.: July 20, 1999.

Information Security: Recent Attacks on Federal Web Sites Underscore Need for Strengthened Information Security Management. GAO/T-AIMD-99-223. Washington, D.C.: June 24, 1999.

VA Information Systems: The Austin Automation Center Has Made Progress in Improving Information System Controls. GAO/AIMD-99-161. Washington, D.C.: June 8, 1999.

Information Security: Many NASA Mission-Critical Systems Face Serious Risks. GAO/AIMD-99-47. Washington, D.C.: May 20, 1999.

Information Security: The Melissa Computer Virus Demonstrates Urgent Need for Stronger Protection over Systems and Sensitive Data. GAO/T-AIMD-99-146. Washington, D.C.: April 15, 1999.

Financial Audit: 1998 Financial Report of the United States Government. GAO/AIMD-99-130. Washington, D.C.: March 31, 1999.

Securities Fraud: The Internet Poses Challenges to Regulators and Investors. GAO/T-GGD-99-34. Washington, D.C.: March 22, 1999.

IRS Systems Security: Although Significant Improvements Made, Tax Processing Operations and Data Still at Serious Risk. GAO/AIMD-99-38. Washington, D.C.: December 14, 1998.

Financial Management Service: Areas for Improvement in Computer Controls. GAO/AIMD-99-10. Washington, D.C.: October 20, 1998.

Federal Reserve Banks: Areas for Improvement in Computer Controls. GAO/AIMD-99-6. Washington, D.C.: October 14, 1998.

Bureau of the Public Debt: Areas for Improvement in Computer Controls. GAO/AIMD-99-2. Washington, D.C.: October 14, 1998.

Financial Management: Improvements Needed in Air Force Vendor Payment Systems and Controls. GAO/AIMD-98-274. Washington, D.C.: September 28, 1998.

Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk. GAO/AIMD-98-92. Washington, D.C.: September 23, 1998.

Information Security: Strengthened Management Needed to Protect Critical Federal Operations and Assets. GAO/T-AIMD-98-312. Washington, D.C.: September 23, 1998.

VA Information Systems: Computer Control Weaknesses Increase Risk of Fraud, Misuse and Improper Disclosure. GAO/AIMD-98-175. Washington, D.C.: September 23, 1998.

Defense Information Superiority: Progress Made, but Significant Challenges Remain. GAO/NSIAD/AIMD-98-257. Washington, D.C.: August 31, 1998.

FAA Systems: Serious Challenges Remain in Resolving Year 2000 and Computer Security Problems. GAO/T-AIMD-98-251. Washington, D.C.: August 6, 1998.

Information Security: Serious Weaknesses Put State Department and FAA Operations at Risk. GAO/T-AIMD-98-170. Washington, D.C.: May 19, 1998.

Computer Security: Pervasive, Serious Weaknesses Jeopardize State Department Operations. GAO/AIMD-98-145. Washington, D.C.: May 18, 1998.

Air Traffic Control: Weak Computer Security Practices Jeopardize Flight Safety. GAO/AIMD-98-155. Washington, D.C.: May 18, 1998.

Executive Guide: Information Security Management: Learning From Leading Organizations. GAO/AIMD-98-68. Washington, D.C.: May 1998.

U.S. Government Financial Statements: Results of GAO's Fiscal Year 1997 Audit. GAO/T-AIMD-98-128. Washington, D.C.: April. 1, 1998.

Financial Audit: 1997 Consolidated Financial Statements of the United States Government. GAO/AIMD-98-127. Washington, D.C.: March 31, 1998.

Financial Audit: Examination of IRS' Fiscal Year 1996 Custodial Financial Statements. GAO/AIMD-98-18. Washington, D.C.: December 24, 1997.

Financial Management: Review of the Military Retirement Trust Fund's Actuarial Model and Related Computer Controls. GAO/AIMD-97-128. Washington, D.C.: September 9, 1997.

Financial Audit: Examination of IRS' Fiscal Year 1996 Administrative Financial Statements. GAO/AIMD-97-89. Washington, D.C.: July 31, 1997.

Small Business Administration: Better Planning and Controls Needed for Information Systems. GAO/AIMD-97-94. Washington, D.C.: June 27, 1997.

Social Security Administration: Internet Access to Personal Earnings and Benefits Information. GAO/T-AIMD/HEHS-97-123. Washington, D.C.: May 6, 1997.

Budget Process: Comments on S.261--Biennial Budgeting and Appropriations Act. GAO/T-AIMD-97-84.

IRS Systems Security and Funding: Employee Browsing Not Being Addressed Effectively and Budget Requests for New Systems Development Not Justified. GAO/T-AIMD-97-82. Washington, D.C.: April 15, 1997.

IRS Systems Security: Tax Processing Operations and Data Still at Risk Due to Serious Weaknesses. GAO/T-AIMD-97-76. Washington, D.C.: April 10, 1997.

IRS Systems Security: Tax Processing Operations and Data Still at Risk Due to Serious Weaknesses. GAO/AIMD-97-49. Washington, D.C.: April 8, 1997.

High Risk Series: Information Management and Technology. GAO/HR-97-9, Feb. 1997.

Information Security: Opportunities for Improved OMB Oversight of Agency Practices. GAO/AIMD-96-110. Washington, D.C.: September 24, 1996.

Financial Audit: Examination of IRS' Fiscal Year 1995 Financial Statements. GAO/AIMD-96-101. Washington, D.C.: July 11, 1996.

Tax Systems Modernization: Actions Underway But IRS Has Not Yet Corrected Management and Technical Weaknesses. GAO/AIMD-96-106. Washington, D.C.: June 7, 1996.

Information Security: Computer Hacker Information Available on the Internet. GAO/T-AIMD-96-108. Washington, D.C.: June 5, 1996.

Information Security: Computer Attacks at Department of Defense Pose Increasing Risks. GAO/AIMD-96-84. Washington, D.C.: May 22, 1996.

Information Security: Computer Attacks at Department of Defense Pose Increasing Risks. GAO/T-AIMD-96-92. Washington, D.C.: May 22, 1996.

Security Weaknesses at IRS' Cyberfile Data Center. GAO/AIMD-96-85R. Washington, D.C.: May 9, 1996.

Tax Systems Modernization: Management and Technical Weaknesses Must Be Overcome to Achieve Success. GAO/T-AIMD-96-75. Washington, D.C.: March 26, 1996.

Financial Audit: Federal Family Education Loan Program's Financial Statements for Fiscal Years 1994 and 1993. GAO/AIMD-96-22. Washington, D.C.: February 26, 1996.

Financial Management: General Computer Controls at the Senate Computer Center. GAO/AIMD-96-15. Washington, D.C.: December 22, 1995.

Financial Management: Challenges Facing DOD in Meeting the Goals of the Chief Financial Officers Act. GAO/T-AIMD-96-1. Washington, D.C.: November 14, 1995.

(310163)